Policy Reference – Central Register	______________________________
Policy Reference – Faculty / Service	**IG 007**
Policy Owner	**Director - Business Assurance**
Date Policy Written	**November 2013**
Date Policy Last Updated	**December 2015**
Date to Information Governance Group	
Date to Audit Committee	
Date for next Review	**March 2017**
Comments	**Updated to include PREVENT references**

1. Introduction

The provision of secure IT systems is a team effort involving the participation and support of every University of Sunderland employee and affiliate who deals with information and/or information systems. It is the responsibility of every computer user to know and adhere to this policy, and to conduct their activities accordingly.

The University of Sunderland has an established culture of openness, trust and integrity, and is committed to protecting all of its employees, partners, students and itself from illegal or damaging actions by individuals, either knowingly or unknowingly.

The purpose of this policy is to outline the acceptable use of computer equipment at University of Sunderland. These rules are in place to protect all types of users of the University IT systems and the University of Sunderland itself. Inappropriate use exposes University of Sunderland to risks including virus attacks, compromise of network systems and services, reputational and legal issues.

2. Scope of the Policy

This policy applies to students, employees, contractors, consultants, temporary/contract, and other staff at the University of Sunderland, including all personnel affiliated with third parties that use University's IT systems or process it's information. This policy applies to all equipment and services owned or leased by University of Sunderland.

IT systems, including but not limited to computer equipment, software, operating systems, storage media, network accounts providing electronic mail, and Internet browsing services, are the property of University of Sunderland. These systems must be used for business purposes in serving the interests of the University, our students, staff and customers in the course of normal operations.

3. Policy Summary

Access to the University's IT systems and services is granted to people with a valid login account. Users of these systems and services must abide by the conditions set out in appendix 1 & 2 of this policy for acceptable and unacceptable use. A summary of unacceptable use is as follows;

- Illegal and unlawful activities including breach of copyright.
- Compromising or circumventing security systems.
- Causing disruption and mischief to IT facilities and services.
- Misuse of electronic messaging and social media services.
- Carrying out unauthorised commercial activities.

Any or all use of the University IT systems and all data held within it may be intercepted, monitored, recorded, copied, audited, inspected, and disclosed to authorised university officials, authorised third parties and law enforcement personnel as part of their duties. In addition, the University operates web filtering on all networks which will include the recording of user details where access to requested web pages are blocked.

Unauthorised or improper use of any University owned or managed system may result in action under the University's disciplinary policies, procedures and regulations and/or civil or criminal penalties.

4. Responsibilities

The Executive member with overall responsibility for this policy is the Deputy Vice Chancellor and Deputy Chief Executive. S/he is responsible for deciding on the outcome of internal reviews of Freedom of Information requests and EIR requests.

The Director of Business Assurance, who performs the role of the University's Senior Information Risk Owner (SIRO) is responsible for:

- Ensuring that an overall culture exists that values and protects information within the organisation
- Owning the organisation's overall information risk policy and risk assessment process, testing its outcome and ensuring that it is used
- Owning the organisation's information incident management framework

The Assurance Manager (Business Assurance - Information Governance), reporting to the Director for Business Assurance, is responsible for drawing up information governance and records management policy, process and guidance and ensuring compliance with this policy.

The Cyber Security Officer (ITS), reporting to the Head of IT Systems, is responsible for developing IT Security policy, standards and guidelines. He/she is also responsible for ensuring that effective IT Security systems, controls and training programs are operationally implemented, fit for purpose and available across the University.

The University Deans of Faculty and Directors of Services have responsibility for ensuring compliance with the University's Information Governance policies and ensuring any issues of non-compliance are addressed. They have responsibility for ensuring that an appropriate member of staff, in each Faculty and Service, is appointed to the role of "Information Champion".

The Information Governance Group is responsible for policy setting and approval and for ensuring policies are followed.

Information Champions are accountable to their Dean of Faculty/Director of Service and have a responsibility to monitor information governance compliance and awareness and be the primary point of contact and source of information and support within the Faculty/Service. The Information Champions Group reports to the Information Governance Group.

Individual students, employees and contractors have responsibility for ensuring that they comply with this policy and any related policies and guidance. Staff must attend training and awareness sessions provided by the University. Employees also have a duty to report any incidents or 'near misses' in relation to information governance.

5. Legislation and related policies

This policy is designed to work in line with current university policy and legislative acts, statutes and best practice guidance such as:

- The Data Protection Act 1998
- Computer Misuse Act 1990
- Copyright, Designs & Patents Act 1988
- Copyright (Computer Programs) Regulations 1992
- PREVENT & Safeguarding Duties
- Janet Connection Policy
- Janet Security Policy
- Janet Acceptable Use Policy

6. Definitions:-

6.1. Policy

A set of policies principles, rules, and guidelines formulated or adopted by an organisation to reach its long-term goals and typically published in a booklet or other form that is easily readable and widely accessible.

6.2. IT System

Information Technology (**IT**) is the application of computers and telecommunications equipment to store, retrieve, transmit and manipulate data, often in the context of a business or other enterprise. The term is commonly used as a synonym for computers and computer networks, but it also encompasses other information distribution technologies such as television and telephones. Several industries are associated with information technology, such as computer hardware, software, electronics, telecom equipment, e-commerce and computer services.

6.3. Network

A computer network is a group of connected computer systems and other computing hardware devices that are linked together through communication channels to facilitate communication and resource sharing among a wide range of users.

7. Acceptable and unacceptable use

University IT facilities are provided to authorised users for the purpose of teaching, learning, research and the normal administrative functions of the University. Occasional personal use of the University's IT facilities is permitted, but such use is a privilege and not a right. Personal use of the University's IT systems must not hinder or interfere with an individuals contractual or professional duties. General terms on acceptable use can be found in Appendix 1. Unacceptable use of the University's IT equipment, services or facilities can be found in Appendix 2.

8. Relationship with other University policies

Anyone wishing to login to the University of Sunderland's IT systems should read and accept this policy in conjunction with the policies listed in Appendix A of the Overarching Information Governance Policy.

Appendix 1 – Acceptable Use

1. General Conditions

While the University of Sunderland desires to provide a reasonable level of privacy, users should be aware that the information they create on the corporate systems remains the property of University of Sunderland. Because of the need to protect University of Sunderland's network and IT infrastructure, management cannot guarantee the confidentiality of information stored on any networked or stand alone IT device belonging to University of Sunderland. Access to the University's IT Systems will be suspended / discontinued upon the termination of employee, student, or affiliate contract. Additionally, access to the University's IT systems may be reduced/restricted while investigations into any breach that may lead to disciplinary action arising from violation of this policy are conducted.

Access to the University IT systems is granted under the following general conditions;

1.1 Authorised users of the University's IT systems are responsible for exercising good judgment regarding the reasonableness of personal use.

1.2 The University information technology and communication facilities, including email addresses and computers, are provided for academic and administrative purposes related to work or study at the University. Very occasional personal use is permitted but only so long as:

1.2.1 it does not interfere with the member of staff's work nor the student's study.

1.2.2 it does not contravene any University policies.

1.2.3 It is not excessive in its use of resources.

1.3 For security and network maintenance purposes, any or all use of the University IT systems and all data held within it may be intercepted, monitored, recorded, copied, audited, inspected, and disclosed to authorised university officials, authorised third parties and law enforcement personnel as part of their duties. The University of Sunderland reserves the right to audit networks and systems, and the information held on them, on a periodic basis to ensure compliance.

1.4 The University operates web filtering on all University networks. As a result, some web pages may be unavailable to users without pre agreed permissions. Records will be retained.

1.5 The information produced and contained on any University IT related system must be classified by the Information Owner as set out in the University's Information Classification policy.

1.6 All users must keep passwords secure and not share accounts. Authorised users are responsible for the security of their passwords and accounts at all times.

1.7 All University owned servers, PCs, mobile devices and workstations must be secured by password protection settings that automatically locks the screen and/or logs the user out after a pre-configured period of inactivity.

1.8 Postings by employees from a University of Sunderland email address to newsgroups should contain a disclaimer stating that the opinions expressed are strictly their own and not necessarily those of the University of Sunderland, unless posting is in the course of business duties.

1.9 All computing equipment connected to the University of Sunderland IT systems, whether owned by an employee, student or the University of Sunderland, must be continually executing approved virus-scanning software with a current virus database.

Appendix 2 – Unacceptable Use

1. General Conditions

The following activities are, in general, prohibited. Under no circumstances is an employee, student or affiliate of the University of Sunderland authorised to use the University's IT systems to engage in any activity that is illegal under national or international law. The list below is by no means exhaustive, but attempts to provide a framework for activities which fall into the category of unacceptable use. The following activities are therefore prohibited;

1.1. Violations of the rights of any person or company protected by copyright, trade secret, patent or other intellectual property, or similar laws or regulations, including, but not limited to, the installation or distribution of "pirated" or other software products that are not appropriately licensed for use by the University of Sunderland.

1.2. Activities which either support or promote extremism or radicalization deemed illegal under UK law. Action will be taken against any individual carrying out or supporting such activities; this may include individuals being reported to the relevant authorities.

1.3. Unauthorised copying of copyrighted material including, but not limited to, digitisation and distribution of photographs from magazines, books or other copyrighted sources, copyrighted music or films.

1.4. The installation of any copyrighted software for which the University of Sunderland or the end user does not have an active license. Exporting software, technical information, encryption software or technology, in violation of international or regional export control laws is illegal. The appropriate management should be consulted prior to export of any material that is in question.

1.5. Introduction of malicious programs such as viruses into the network, server, desktop or mobile devices.

1.6. Revealing your account password to others or allowing use of your account by others. In the case of staff this includes family and other household members when working at home.

1.7. Using any University of Sunderland's IT systems to actively engage in procuring or transmitting material that is in violation of sexual harassment or hostile workplace laws.

1.8. Using the University's computing services to conduct any form of unauthorised commercial activity not related to the University's business.

1.9. Making fraudulent offers of products, items, or services originating from any University of Sunderland account.

1.10. Process or store any payment card data on any system, computer or transmit via the network unless authorised to do so.

1.11. Effecting security breaches or disruptions of network communication. Security breaches may include, as an example, but are not limited to:

1.11.1. Accessing data of which the employee, student or affiliate is not an intended recipient.

1.11.2. Logging into a server or account that the employee, student or affiliate is not expressly authorised to access, unless these duties are within the scope of regular duties. For purposes of this section, "disruption" indudes, but is not limited to, network sniffing, pinged floods, packet spoofing, denial of service, and forged routing information for malicious purposes.

1.11.3. Network Port scanning or security scanning of the University computer network.

1.12. Executing any form of network monitoring on the University network, which will intercept data, not intended for the employee, student or affiliate.

1.13. Circumventing user authentication or security of any University of Sunderland's IT equipment or services.

1.14. Interfering with or denying service to any or all users of University of Sunderland IT equipment and services, including the services themselves.

1.15. Using any program/script/command, or sending messages of any kind, with the intent to interfere with, or disable, a user's login session, via any means, locally or via the Internet or Intranet.

1.16. Providing information about, or lists of, University of Sunderland employees, students and affiliates to parties outside University of Sunderland unless the role of the individual defined by the University requires it.

2. Unacceptable Use - Email and Communications

The following activities are prohibited. Under no circumstances is an employee, student or affiliate of the University of Sunderland authorised to use the University's IT systems to engage in any activity that is illegal under national or international law.

The list below is by no means exhaustive, but attempts to provide a framework for activities, which fall into the category of unacceptable use. The following activities are therefore prohibited;

2.1. Sending unsolicited email messages, including the sending of "junk mail" or other advertising material to individuals who did not specifically request such material.

2.2. Any form of harassment via email, telephone or paging, whether through language, frequency, or size of messages.

2.3. Unauthorised use, or forging, of email header information.

2.4. Solicitation of email for any other email address, other than that of the poster's account, with the intent to harass or to collect replies.

2.5. Posting the same or similar non-business-related messages to large numbers of Usenet newsgroups (newsgroup spam).

2.6. Employees and students must not open e-mail attachments received from unknown senders, which they suspect may contain viruses. If in doubt a service request should be raised via the internal IT Service Desk on extension 3333 or via the IT Portal at https://itportal.sunderland.ac.uk.

3. Unacceptable Use - Internet

Internet usage is granted for the sole purpose of supporting the business of the University of Sunderland and student learning activities. All users of the Internet should be aware that the University's network creates an audit log for both in-bound and out-bound addresses, and is periodically reviewed. Internet access will be discontinued upon termination of employee, student, or affiliate contracts or disciplinary action arising from violation of this policy.

The list below is by no means exhaustive, but attempts to provide a framework for activities, which fall into the category of unacceptable use and are therefore prohibited;

3.1. The use of its Internet service for political activity, engaging in any form of intelligence collection, engaging in fraudulent activities, or knowingly disseminating false or otherwise libellous materials.

3.2. The use of its Internet Service for the purposes of supporting terrorism or activities supporting radicalisation

3.3. Any conduct that would constitute or encourage a criminal offense, lead to civil liability, or otherwise violate any regulations, national or international law.

3.4. Use, transmission, duplication, or voluntary receipt of material that infringes on the copyrights, trademarks, trade secrets, or patent rights of any person or organisation. All users must assume that all materials on the Internet are copyright and/or patented unless specific notices state otherwise.

3.5. Transmission of any proprietary, confidential, or otherwise sensitive information without the proper controls.

3.6. Creation, posting, transmission, or voluntary receipt of any unlawful, offensive, libelous, threatening, harassing material, including but not limited to comments based on race, national origin, sex, sexual orientation, age, disability, religion, or political beliefs.

3.7. Unauthorised downloading of any shareware programs or files that may harm the University's IT infrastructure and/or cause service disruption.

3.8. The University of Sunderland supports strict adherence to software vendors' license agreements. The University IT computing and networking resources must not be used for the copying of software in a manner not consistent with the vendor's license agreement. Questions regarding lawful versus unlawful copying should be referred to the IT Security Manager for review or to request a ruling from the Legal Department before any copying is done.

Internet access via the University of Sunderland's network is provisioned only to devices that have been registered via an approved login. Under no circumstances should users share the Internet connection to other non-authorised users or non-registered devices.