University of Sunderland
Technical Services
Cyber Security and Information Governance
Policy Document
Classification – Public

IT Regulations and Acceptable Use Policy (IG007)	
Version Number:	1.0
Policy Reference:	IG 007
Policy Owner:	Technical Director
Date Written:	November 2015
Date of Last Update:	April 2019
Author:	Cyber Security & Information Governance Team
Approval Route:	Technical Services to Operations Board.
Date Approved:	April 2019
Next Review:	November 2020
Comments:	Approved

1. INTRODUCTION AND PURPOSE

Who is this for?

Everyone who uses the University of Sunderland's Computers, Systems, and/or Network services.

What is expected?

Know the rules
✓ Understand the relevant Law, so you don't break it.
✓ Abide by the University Regulations, Policies, and Guidance.
✓ Observe the regulations of any third parties whose facilities you access.

We want to give you the best information and guidance available, to keep you, and the University safe and informed on how to use the systems you have access to.

2. SCOPE

This guidance applies to everyone at the University of Sunderland, and to all equipment and services owned, leased or operated by, or on behalf of, the University of Sunderland.

IT systems, are the property of the University, to be used for University business purposes.

Personal use is a permitted privilege. However, you are encouraged to use your own equipment for personal use where possible. Please note that whilst personal use is permitted, University owned and managed services and equipment should not be used to store documents and data that are personal to you. The University cannot be held responsible for the security, backup and recovery of such data in the event of this data being corrupted, inappropriately accessed or lost.

3. POLICY SUMMARY

Access to the University's IT systems and services is granted only to specific, authorised people. Users of these systems and services must abide by the conditions set out in IT Regulations and Guidance notes to this policy for acceptable and unacceptable use.

For security and network maintenance purposes, any or all use of the University IT systems and all data held within them 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, fault-find, and maintain networks and systems, and the information held on them, on a periodic basis.

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

User activity log information will be retained, and may be used for purposes, including, but not limited to;

- Network monitoring;
- Cyber security;
- Operational management; and
- Safeguarding;
- As a requirement of the PREVENT duty.

The logged information includes;

- Firewall traffic and website access logs;
- Details of the user identity (where available);
- Source and destination IP addresses;
- The type of traffic;
- Intrusion prevention information;
- Website classification.

In the event of a User's account credentials being found to be used for malicious purposes or after repeated failed attempts to access systems, those credentials may be reset, in order to protect the data, information and systems normally accessed by using the credentials.

Postings by employees from a University of Sunderland email address to newsgroups and/or social media 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.

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, and set to be patched automatically, unless specifically authorised otherwise in writing from the University's Technical Director.

4. PRINCIPLES OF ACCEPTABLE USE

Be yourself

✓ Keep your account details secure. Never reveal your password.
✓ Keep passwords safe. Create secure passwords.
✓ Use different passwords for each account, so others can't guess or reuse them elsewhere.
✓ Change passwords if you suspect any actual or potential compromise of your account.
✓ Use your own identity online. Don't pretend to be anyone else.
✓ Use your own account. Never use anyone else's. Don't let anyone use yours.

Use facilities appropriately

✓ Use your own equipment for personal use.
✓ Allow system updates to complete, (help to keep everyone's systems safe).
✓ Use properly licenced software, up-to-date with updates set to automatically install.
✓ Use Multi-Factor Authentication wherever available.
× Don't do anything that increases the risk of malware affecting IT systems and devices.
× Don't interfere with hardware or load unauthorised software on University devices.

Behave respectfully

✓ Behave respectfully towards other people.
✓ Treat Information with respect, dispose of it appropriately when no longer required.
× Don't waste IT resources or interfere with other users' legitimate use.
× Don't behave in a way that is unacceptable to others in the physical world.

Be aware of your footprint

× Don't put it on-line if it doesn't need to be on-line. If it does need to be on-line, manage it.

- Data stays online for a very long time, will it still be appropriate in 10 years?
- All data stored within the university may be searched and disclosed for Subject Access Requests, Freedom of Information and Environmental Information Regulations requests.
- University services, systems and networks are subject to monitoring for the purposes of system security, data security, system assurance and official investigations.

Report issues you see

✓ If something does not feel correct, check it with the IT service desk. Acting on an issue through early reporting can reduce damage and minimise clean-up time/cost.
✓ If you don't know how to do something, ask, we want to help you get things right.
✓ Be the person who prevents something small becoming a bigger issue.

Exercise good judgement

✓ Be reasonable concerning the posts and comments you make.

5. QUESTIONS TO ASK YOURSELF CONCERNING GOOD JUDGEMENT

? Is it important for me to comment?

- Exercise good judgment regarding the reasonableness of posts and comments you make online towards other people. If you're not comfortable being the subject of a similar comment, don't comment in that way about others.

? Could my comment be misconstrued or offence be taken from what I have said?

- Exercise good judgment regarding the reasonableness of comments you make about the university, its staff and other people, to prevent attracting accusations of harassment or defamation. Don't make unreasonable comments about activity, people or behaviours. Treat others with dignity and respect.

? Is it appropriate for me to comment publically?

- People may not have exercised good judgement on-line and sometimes it may be better to not respond, allowing the dust to settle and not jumping to conclusions. It may be more prudent to check understanding by speaking with an individual in person, or by phone rather than posting on-line. You may be able resolve matters without leaving an online footprint for anyone to review in years to come.

? Am I comfortable for my postings to be officially discovered in the future?

- Documents and comments stored online are retained, copied and redistributed, making them practically impossible to be removed. They can be referenced within the media and potentially within law courts or employment tribunals.
- When a Subject Access Request is received, the University could be asked for "all correspondence relating to subject x,y,z", which will result in a review of all relevant content and communication trails. The discovered material will be released to the requester, even if users have not previously used good judgement on that occasion).

? Am I happy for my on-line content to reach those I didn't intend?

- Facebook, Instagram and other services are excellent sources for people wanting to find out about you. Such content is likely to be accessed by people it wasn't meant for and they will form judgements about you based on your posted activity. Past Facebook images, Linked-In comments and twitter posts may well be taken into consideration by hiring managers when recruiting potential employees. It's very easy to search for a name on-line during a CV review and decide to avoid a person based on past postings and old images. You cannot control on-line search engines.

? Am I diligent enough before clicking to access something?

- Employees and students must not open e-mail attachments received from unknown senders, unless they are certain that the content of the attachment is not malicious. Employees and students must avoid clicking on links or content which they suspect may contain viruses, because they are from an unknown source, or from a known source but with an unexpected label, or are of an unexpected or unusual nature.
- If you suspect an email is spam and feel it should be reported, please forward it to spam@sunderland.ac.uk and cyber@sunderland.ac.uk, then delete the message. If you believe it is necessary, or are in doubt, raise a service request via the UIT Service Desk on extension 3333 or via the IT Portal at https://itportal.sunderland.ac.uk.

The Student Handbook has advice and guidance for students on use of social media, available at https://my.sunderland.ac.uk/

6. RELEVANT POLICIES & LEGISLATION

The policies, regulations, and guidance are designed to ensure that we as a University work in line with current legislative requirements;

Anyone wishing to login to the University of Sunderland's IT systems should read, understand, and accept this policy in conjunction with the policies listed.

Policies of particular relevance are available at https://ts.sunderland.ac.uk/ and include:

- Data Protection Policy
- Employment contracts & requirements (via HR)
- IT Regulations and Acceptable Use Policy, (This document)
- IT Regulations and Acceptable Use Guidance
- Information Security Policy
- Network Monitoring, Security and Interception Guidance
- Records Management Policy
- Student Regulations

Legislation of relevance is available at www.legislation.gov.uk and includes:

- The Data Protection Act 2018, incorporating General Data Protection Regulation, (EU) 2016/679
- Computer Misuse Act 1990
- Copyright, Designs & Patents Act 1988
- Copyright (Computer Programs) Regulations 1992
- Counter Terrorism and Security Act 2015 (including the PREVENT duty)
- Criminal Justice and Immigration Act 2008
- Obscene Publications Act 1959

JaNET Requirements are available at https://community.jisc.ac.uk/library/janet-policies:

- Janet Acceptable Use Policy
- Janet Connection Policy
- Janet Network Monitoring & Interception Policy
- Janet Security Policy

Proposed Legislation, due to be enacted prior to the next policy review:

- Digital Economy Act 2017, incorporating Age Verification Regulations (from April 2019).
- The Directive on Copyright in the Digital Single Market 2016/0280(COD) as Implemented by UK enabling Legislation (Content Blocking).

Available at https://ts.sunderland.ac.uk/csig/legislation.

7. DEFINITIONS

7.1. Policy

A set of policies, principles, rules, and guidelines formulated or adopted by an organisation to reach its long-term goals, easily readable and widely accessible.

7.2. Network

A computer network is a group of connected systems and devices that are linked together to facilitate communication and resource sharing among users of the network.

7.3. Guidance Note

A document allowing further explanation and communication to Users and Staff, about the method of implementation of policies and procedures, the roles, processes, and accountability associated with a particular policy, to aid transparency and understanding of how it is implemented within the organisation.

Provided to Users for information, to enable them to be better informed about how policies translate into operation and which safeguards in place.

7.4. Appendices to IT Regulations

A document allowing further explanation and communication to Users and Staff, about the full IT Regulations, specifying what is and is not Acceptable Use in different circumstances.

8. RESPONSIBILITIES

The **Executive Member** with overall responsibility for the operation of this policy is the Chief Operating Officer (COO).

Individual students, employees, contractors, consultants, partners, temporary/contract staff, third parties have responsibility for ensuring that they comply with this policy and any related policies and guidance. **Users** of the service and **Staff** of the University must attend training and awareness sessions provided by the University. **All Users** also have a duty to report any incidents or 'near misses' in relation to Cyber Security and/or Information Governance to the IT Service Desk.

ENDS