Student AUP* Code of Practice

(*ICT Acceptable Use Policy)

Effective from 13 January 2014

Version Number: 3.0

Author: Senior Information Security officer
Governance Services Unit
Code of Practice Management and Responsibilities

Owner: This Code of Practice is issued in support of the ICT AUP V 4.0 by the Executive Director of ITS, (Chief Information Officer (CIO)) and the University Secretary. The CIO has the authority to issue and communicate policy on University ICT facilities, services and usage. The University Secretary responsibilities include Information Governance functions within GSU. All students must comply with this Code of Practice and the full ICT AUP.

Others with responsibilities (please specify):

Assessment

<table>
<thead>
<tr>
<th>Equality Analysis</th>
<th>Cross relevant assessments</th>
<th>Cross if not applicable</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Legal</th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Information Governance</th>
<th>X</th>
<th></th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>Academic Governance</th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Consultation

<table>
<thead>
<tr>
<th>Staff Trades Unions via HR</th>
<th>Cross relevant consultations</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Students via USSU</th>
<th>Cross relevant consultations</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Any relevant external bodies (please specify) Cross if not applicable

Authorised by: University Secretary & ITS Executive Director

Date authorised: 17 December 2013

Effective from: 13 January 2014

Review due: 2 years by January 2016

Document location:
e.g. University Policy & Procedures page: www.salford.ac.uk/university/governance/policies-and-procedures

Document dissemination and communications plan
As per ICT Acceptable Use Policy V4.0 (which this document summarises for Students)
1.0 Purpose and Scope

The ICT Acceptable Use Policy (AUP) applies to all students. It details acceptable and prohibited ICT activity. All ICT usage is automatically logged and may be monitored. This is just a guide, you are still bound by the full AUP.

2.0 Code of Practice Statements

2.1 In particular you must not

- Use file sharing (peer to peer / p2p) software, such as torrent, to download or upload material protected by copyright law (including music, films, games and software)
- Connect any computer to the University’s networks without a regularly updated operating system and updated antivirus software installed
- Download and/or post illegal, pornographic, discriminatory or offensive material
- Make, install or distribute illegal copies of computer software
- Connect any form of networking device such as wireless access points, routers or hubs to the University’s networks
- Send or forward any junk mail or spam
- Use any hacking tools
- Run any sort of server or server based services without permission

When on social media web sites: consider your reputation and that of the University.

2.2 Protect your password

Protect your username and password (login, filestore, blackboard and internet) - you are responsible for all activity that takes place under your login details, so don’t share them.

- Use a combination of at least 8 letters, numbers and symbols that you must not tell anyone and don’t need to write down. Try using a memorable saying or phrase e.g. My best friend’s birthday is April 4 - buy gift! = MbfbiA4-bg!

- You’ll also need to protect you Student Email account and password, and your Athens password. Contact the Service Desk if you need any help. Tel:0161 2952444 or email its-servicedesk@salford.ac.uk

- If you are worried someone has guessed your University account password, press Ctrl, Alt and Delete keys, whilst logged on in a campus PC Suite to change your password. You can also use these keys to log off and shut down the computer.

- The University of Salford will never ask you to reveal any passwords via email, or send phishing or ‘threatening’ messages insisting you change passwords – these are attempts by fraudulent people to steal your identity and financial details. Do not respond to such emails, just delete them.

2.3 Protect yourself – personal security

Follow the advice leaflet on physical and personal safety: http://www.advice.salford.ac.uk/page/security
Report Security concerns to Estates Security Control (24/7) on 0161 2954773.

2.4 Protect your personal computer
You can help protect the University network and information by protecting your personally owned computer, laptop or tablet (PC and Mac). Viruses and spyware can infect and slow your computer, steal your identity and your money. You should set regular updates for anti-virus, operating system and anti-spyware software as well as weekly scans.

1) If you are in Halls of Residence, the Clean Access Agent will help you to set the necessary updates. Ensure you also set a weekly scan of your computer for viruses.

2) If you are not in Halls, but use a computer on the internet you should set the updates on your computer yourself.

2.5 Saving your work

Your personal space on the University ICT network is known as your F: drive. It is unique to your username. If you save to other devices or locations, just remember where you put what and keep backup copies – once it’s gone, it’s gone! Guidance is also available on the Microsoft Office 365 which offers large storage capacity linked to your student email account. http://www.its.salford.ac.uk/students/email/

2.6 Copying & Copyright

Please be aware that copyright laws apply to all library, e-library material as well as material on the internet. See posters next to every Library photocopier and check the Information Governance website at http://www.infogov.salford.ac.uk/copyright/

3.0 Code of Practice Enforcement

3.1 Failure to follow the AUP may result in

- Blocking of your University computer account and ID Card access
- Reconnection fee of £100 for ICT AUP breaches
- Punishment under the Student Discipline Procedure
- Disconnection & seizure of equipment that is in violation of the policies

The full ICT AUP is available at:
http://www.salford.ac.uk/about-us/corporate-information/governance/policies-and-procedures/browse-by-theme/8

3.2 If your University IT account has been blocked - What to do next

If your IT account has been blocked, you will need to contact a member of the ITSERT team to discuss the matter (arranged via ITS Service Desk).

Following an AUP breach, you must stop that activity and/or remove the offending software from your computer and contact the Finance Department at Faraday House to pay the £100 AUP reconnection fee on your student finance record.

IT and Library access will normally be re-activated within 24 hours of your discussion with an ITSERT member. However if the case is more serious, it may lead to disciplinary action.