Internet Acceptable Use Policy

Policy for acceptable use of Internet access

An Open University Information Security Common Policy

Open University – Information Security Team

Information Classification: Internal use only
Purpose
This policy defines the acceptable use of OU Internet facilities; to protect the OU’s information systems.

Overview
The Internet Acceptable Use Policy covers general secure practice for the use of Open University supplied internet facilities and should be read in conjunction with the other IT Security Policies.
Technical terms used within this document are defined in Appendix A.
It is the responsibility of every computer and information user to know and follow this policy.

Scope
All users of OU information and information systems with the exception of the use of publicly accessible externally presented systems.

Policy
1. General Principles
1.1 Use of the Internet is permitted and encouraged to support the goals and objectives of The OU. The Internet is to be used in a manner that is consistent with the Open University’s ‘Behaviours and Standards at Work’ policy available on the HR website.

2. Personal Use
2.1 Incidental and occasional personal use of the Internet is permitted, subject to the restrictions contained in this policy. Personal use of the Internet must not detrimentally affect the performance of other employees, disrupt the system and / or harm The Open University’s reputation.

3. Internet usage
The following activities are prohibited unless they are a specific requirement of your role:

3.1 Downloading any software or files without Open University approved virus protection measures.
3.2 Downloading any software unless your job specifically requires this and such downloads are fully licenced.
3.3 Visiting hacking sites or downloading hacking or evidence eliminating software.
3.4 Intentionally visiting or downloading material from internet sites that are likely to contain obscene, racist, hateful or other objectionable materials
3.5 Downloading password recovery, cracking, security analysis or any other security software unless explicitly authorised by the Head of IT Security.

3.6 Intentionally interfering with the normal operation of the systems, including the propagation of computer viruses.

3.7 Causing sustained high volume network traffic that substantially hinders others in their use of the network (Examples include web streaming such as MTV or sports sites).

4. Monitoring and Blocking

4.1 The Open University may use software tools to block sites that are obscene, hateful or have other objectionable materials or may affect the university’s operations.

4.2 For security and maintenance purposes, authorised individuals within the Open University central IT teams may monitor all data, systems and network traffic at any time to ensure compliance with this and other security policies and the effective operation of the University’s systems.

5. Enforcement

5.1 Any breach of these policies is significant as it may undermine the effective running of the Open University and its ability to meet its duties and legal obligations. Failure to comply may lead to disciplinary action, including dismissal for serious or repeated breaches. It may also be the case that your conduct and/or action(s) may be unlawful. The Open University reserves the right to inform the appropriate authorities in such cases. You should note that you may be personally liable for actions and or conduct arising from the use of Open University Systems.
### Appendix A - Definitions

<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Internet facilities</td>
<td>Access to the Internet whilst connected to the Open University network. Typically accessed through a web browser to access internet web sites, but can equally be used to access internet resources and services.</td>
</tr>
<tr>
<td>Hacking</td>
<td>The unauthorised access to or use of data, systems, servers or networks, including any attempt to probe, scan or test for vulnerabilities or to breach security or authentication measures without express authorisation of the owner.</td>
</tr>
</tbody>
</table>