



# Blacklisting Procedure UNDER REVIEW

---

<b>Related Policy</b>	ICT Services and Facilities Use Policy
<b>Responsible Officer</b>	Chief Information Officer
<b>Approved by</b>	Chief Information Officer
<b>Approved and commenced</b>	August, 2014
<b>Review by</b>	August, 2017
<b>Responsible Organisational Unit</b>	Information Technology Services

---

## CONTENTS

1	Objective .....	2
2	Scope .....	2
3	Procedure.....	2
4	Definitions and Acronyms .....	3
5	Supporting Documentation .....	5
6	Versioning .....	5

## 1 Objective

This procedure describes the process the University of Tasmania will follow in restricting access to online services or websites where accessing, or obtaining content from, those services or websites using University of Tasmania ICT Services, Facilities or Infrastructure would be considered a breach of Federal or State legislation, or a breach of University of Tasmania Policy.

## 2 Scope

Where the blockage of an online service, or website, affects learning, teaching, research or general work the blockage will be reviewed and may be removed, or be subject to a per user, or group, exception.

## 3 Procedure

<b>Step</b>	<b>Details</b>	<b>Responsibility</b>
1.	<p>An internet service, or website, may be blacklisted if accessing, or obtaining content from that service or website using University of Tasmania ICT Services, Facilities, or Infrastructure would be considered a breach of Federal or State legislation, or a breach of University of Tasmania Policy.</p> <p>Blacklisting any internet service, or website, may only be done by the process of:</p> <ul style="list-style-type: none"> <li>• nomination of an internet service or website</li> <li>• consideration by the Chief Information Officer and subsequent approval</li> <li>• configuration change to centralised systems</li> <li>• instantiation of a review process.</li> </ul>	Chief Information Officer
2.	<p>Internet services, or websites, that are candidates for blacklisting may be identified by:</p> <ul style="list-style-type: none"> <li>• consistent association with cases of Policy breach;</li> <li>• nomination by ICT Officers; or</li> <li>• identification in the course of operational work.</li> </ul>	ICT Security Manager, ICT Officer
3.	<p>A nominated internet service, or website, will be considered for blacklisting by the Chief Information Officer.</p> <p>The Chief Information Officer, will take into consideration:</p> <ul style="list-style-type: none"> <li>• nature of content hosted on the nominated internet service or website. Including: <ul style="list-style-type: none"> <li>○ Legality under Federal and State legislation</li> <li>○ Legality under University of Tasmania Policy</li> </ul> </li> <li>• use for learning, teaching, research or general University work.</li> </ul>	Chief Information Officer

The Chief Information Officer, will approve/disapprove the blacklisting of any internet service or website following this assessment.

Following approval of an internet service or website for blacklisting the Chief Information Officer will notify the ICT Security Manager.

- |    |  |                      |
|----|--|----------------------|
| 4. | The ICT Security Manager will arrange for a configuration change to the University's internet gateways or firewall to facilitate the blacklisting. | ICT Security Manager |
|----|--|----------------------|

The University Service Desk and ICT Officers will be notified of the blacklisted internet service or website via email.

- |    |   |                  |
|----|---|------------------|
| 5. | Where blacklisting a website impacts learning, teaching, research, or University work any Authorised User may request a review of a decision to blacklist a site, which may be directed to the Chief Information Officer or the ICT Security Manager. | Authorised Users |
|----|---|------------------|

Requests to review a decision to blacklist a site will be accepted by email, or escalation via an ICT Officer.

Any request to review a decision to blacklist a site should include details of the access requirements and a summary of the University business associated with it.

- |    |  |                           |
|----|--|---------------------------|
| 6. | The Chief Information Officer will consider the review request and apply any of the following actions:   | Chief Information Officer |
|    | <ul style="list-style-type: none"> <li>• removal of the internet service or website from the blacklist</li> <li>• a per user access exemption</li> <li>• access exemption for a group of users, or department, based on network addresses</li> <li>• no access exemption.</li> </ul> |                           |

- |    |  |                      |
|----|--|----------------------|
| 7. | A register of blacklisted internet services and websites will be maintained. In addition, a register of exceptions will be maintained. | ICT Security Manager |
|----|--|----------------------|

#### 4 Definitions and Acronyms

- |               |  |
|---------------|--|
| <b>Access</b> | <p>Connection of University, personal or third party owned Devices to ICT Infrastructure facilities via a direct or indirect connection method. Such connection methods could include but are not restricted to:</p> <ul style="list-style-type: none"> <li>• LAN/MAN/WAN network connections (e.g. Ethernet);</li> <li>• Wireless network connections;</li> <li>• Remote access via a third party such as a contracted</li> </ul> |
|---------------|--|

	<p>ISP with trusted access to the University network;</p> <ul style="list-style-type: none"><li>• Connection via VPN (Virtual Private Networking) technology; and</li><li>• Connection to any systems, services and applications.</li></ul>
<b>Account</b>	<p>A combination of a username (identifier) and password allocated by an ICT Officer to an Authorised User (the account owner) to access ICT Services, Facilities and Infrastructure.</p>
<b>Authorised User</b>	<p>An individual who has been granted access to University ICT Services under one or more of the following categories:</p> <ul style="list-style-type: none"><li>• a current member of the governing body of the University;</li><li>• a currently employed officer or employee of the University;</li><li>• a currently-enrolled student of the University;</li><li>• any person granted access to use University of Tasmania ICT Services including, but not limited to:<ul style="list-style-type: none"><li>▪ A contractor undertaking work for the University under the provisions of a legal contract;</li><li>▪ A member of a collaborative venture in which the University is a partner; or</li><li>▪ A visiting lecturer, student or other associate who is undertaking similar activities in a recognised University, as a registered associate.</li></ul></li></ul>
<b>Copyright</b>	<p>A form of intellectual property which gives the creator of an original work exclusive rights in relation to that work; and control over its distribution, publication, and adaption.</p>
<b>ICT</b>	<p>Information and Communication Technologies</p>
<b>ICT Facilities</b>	<p>All computers, terminals, telephones, end host devices, licences, centrally managed data, computing laboratories, video conference rooms, and software owned or leased by the University.</p>
<b>ICT Infrastructure</b>	<p>All electronic communication devices, networks, data storage, hardware, and network connections to external resources such as AARNet and the Internet.</p>
<b>ICT Officer</b>	<p>The University of Tasmania staff authorised by the Faculty, School and/or Director, IT Services to maintain and/or administer ICT Services, Facilities, Infrastructure, user level accounts and passwords.</p>
<b>ICT Security Manager</b>	<p>The ITS appointed representative responsible for ICT security.</p>

<b>ICT Services</b>	All systems supporting interaction, information provision, information storage, or communications provision and the ICT Facilities on which they operate.
<b>Internet</b>	<p>A term for the global computer network used to share information along multiple channels, and over multiple protocols.</p> <p>This definition of Internet is inclusive of protocol driven networks such as the World Wide Web, and all peer-to-peer networks.</p>
<b>ITS</b>	Information Technology Services
<b>University</b>	The University of Tasmania

## 5 Supporting Documentation

- ICT Security Policy
- ICT Services and Facilities Use Policy
- ICT Access Control Policy

## 6 Versioning

<b>Former Version</b>	Blacklisting Procedure, approved May, 2010; reviewed May, 2014.
<b>Current Version</b>	Blacklisting Procedure; minor amendments to update changes to terms; approved Responsible Officer, Chief Information Officer, August, 2014.