

GA 41. Websites Filtering Policy

Title:	Websites Filtering Policy
Policy Number:	GA 41/ 07.18
Effective Date:	July 24, 2018
Approval and Review:	Revised and approved on October 22, 2024
Issuing Authority:	VP for Development

1. RATIONALE

Web content filtering is an automatic system that blocks content according to a subscription-based website categorization and reputation.

2. POLICY

Web content filtering is an automatic system that blocks content according to a subscription-based website categorization and reputation.

When a student attempts to visit a website, the University's web content filter checks the category of the site based upon a knowledgebase. The University has implemented access blocking to sites categorized as:

- Adult Content/Adult Material/Sexual Content
- Bot Networks, Keyloggers, Malicious Web Sites, Phishing and other Frauds, Spyware
- Cheating
- Gambling
- Hacking, Proxy Avoidance
- Illegal or Questionable
- Peer-to-Peer File Sharing
- Racism and Hate
- Violence
- Weapons

If a website is blocked by the Internet content filtering system, you will be redirected to a screen advising you that the site has been filtered and the prohibited category the site belongs to.

RHU's Internet content filter assists staff, faculty and students by blocking access to compromised sites to prevent infection of their computers. The University has no control over legitimate web sites that have been compromised, and subsequently categorized as a "Malicious Web Site".

Requests for web sites to be re-categorized from "Malicious Web Site" to another category cannot be accepted, as they will compromise security controls on Curtin's environment.

For other "incorrect" categories you can request the category of the site be reviewed. If a site is reviewed and re-categorized, RHU's Internet content filter database is updated. The average turnaround time for this is within 24 hours.

3. RELATED DOCUMENTS

- > IT Manual