Technology Services
Policy Document

UNIVERSITY OF CUMBRIA

INTERNET CONTENT FILTERING POLICY

Technology Services

NB. This policy is available on the University of Cumbria website and it should be noted that any printed copies are uncontrolled and cannot be guaranteed to constitute the current version of the policy.

POLICY SCHEDULE	
Policy title	Internet Content Filtering Policy
Policy owner	Head of Technology Services, Stephen Young
Policy lead contact	Head of Technology Services, Stephen Young
Policy Number	POL002
Approving body	Business Assurance Board
Date of approval	26 June 2021
Date of implementation	26 June 2021
Version no.	1.2

Related Guidelines, Procedures, Codes of Practice etc.	JANET (UK) Acceptable Usage Policy - covers all users of the JANET network. Safeguarding Vulnerable Groups Information Security Policy Social Media Policy HM Government Prevent Duty Guidance 2015 E-Safety Policy
Review interval	Annual

Document Information

Scope

This policy applies to all staff and students at the university.

It also applies to partners, visitors and guests of the university using the university infrastructure.

Document history

Version	Date	Author	Comments
1.0	12/10/2020	Stephen Young	Creation
1.1	07/04/2021	Stephen Young	Updated Exemption process following IT Advisory Group (March 2021).
1.2	25/05/2021	Stephen Young	Table re-formatting, added 'Plagiarism' to staff allowed and updated exemptions to included reference to Research.

Contents

1. Summary

The University prohibits (blocks/filters) access to certain internet content based upon a series of categories. Web protection is designed to prevent inadvertent unsafe or illegal access, damage or embarrassment. Any restrictions are designed to both record-attempted access and block the majority of sites considered:

a) a cyber security threat to the university, its staff, students or guests,
b) inappropriate or unacceptable,
c) of a radicalised nature / promoting terrorism (under the University's Prevent duty under the Counter-Terrorism and Security Act 2015)

Restrictions are not implemented to restrict academic freedom.

It is acknowledged that the definition of 'inappropriate' or 'unacceptable' will vary according to an individual or a group. Therefore, the implementation of this Policy must be based on agreed university values.

2. Categories

The main categories addressed within the Internet Content Filtering Policy are:

- drugs - For example, websites that sell illegal/controlled substances, promote substance abuse or sell related paraphernalia.

- gambling – For example, on/offline gambling and websites that promote gambling skills and practice.

- hate and discrimination - For example, websites that promote aggressive, degrading, or abusive opinions about any section of the population on the basis of an individual's race, religion, gender, age, nationality, physical disability, sexual preferences or any other lifestyle choice.

- pornography and adult material - For example, websites containing sexually explicit content.

- security / cyber threat – For example, websites site hosting malware/phishing/viruses

- violence - For example, websites that display or promote content related to violence against humans or animals.

- terrorism and extremism - For example, websites promoting terrorist activities, radicalisation or extremism.

The university uses multiple technologies to automatically prevent access to websites in the above categories known to be a problem or known to be illegal. As all network access is treated equally, the minimum tolerance level for protection has to be provided to adequately protect our most vulnerable groups or statutory requirements.

Internet Content categories and their levels of access are set out below. Two 'global' lists are managed to either allow or block sites should incorrect categorisation occur.

Key

X: Blocked **✓:** Allowed

Categories		**Status**		
Category	**Subcategory**	**Staff**	**Student**	**EduRoam and Visitor/Guests (BYOD)**
Potentially Liable	**Child Abuse**	**X**	**X**	**X**
	Discrimination	**X**	**X**	**X**
	Drug Abuse	**X**	**X**	**X**
	Explicit Violence	**X**	**X**	**X**
	Extremist Groups	**X**	**X**	**X**
	Hacking	**X**	**X**	**X**
	Illegal or Unethical	**X**	**X**	**X**
	Plagiarism	✓	**X**	**X**
	Proxy Avoidance	**X**	**X**	**X**
Adult/Mature	**Abortion**	✓	✓	✓
	Advocacy Organizations	✓	✓	✓
	Alcohol	✓	✓	✓
	Alternative Beliefs	✓	✓	✓
	Dating	✓	✓	✓
	Gambling	**X**	**X**	**X**
	Lingerie and Swimsuit	✓	✓	✓
	Marijuana	**X**	**X**	**X**
	Nudity and Risqué	✓	✓	✓
	Other Adult Materials	**X**	**X**	**X**
	Pornography	**X**	**X**	**X**
	Sex Education	✓	✓	✓
	Sports Hunting and War Games	✓	✓	✓
	Tobacco	✓	✓	**X**
	Weapons (Sales)	✓	✓	✓
Bandwidth Consuming	**File Sharing and Storage**	✓	✓	✓
	Freeware and Software Downloads	✓	✓	✓
	Internet Radio and TV	✓	✓	✓
	Internet Telephony	✓	✓	✓
	Peer-to-peer File Sharing	**X**	**X**	**X**
	Streaming Media and Download	✓	✓	✓
Security Risk	**Dynamic DNS**	✓	✓	✓
	Malicious Websites	**X**	**X**	**X**
	Newly Observed Domain	✓	✓	✓
	Newly Registered Domain	✓	✓	✓

	Phishing	**X**	**X**	**X**
	Spam URLs	**X**	**X**	**X**
General Interest - Personal	**Advertising to Entertainment to Shopping and Travel**	✓	✓	✓
General Interest - Business	**Charitable Organisations to Finance and Banking to Online Meetings and search Engines**	✓	✓	✓

3. Exemptions and site ‘white listing’

Where academic or business needs conflict with university filtering policy, exceptions can be made to support access to specific sites. This could be for specific cohorts or academics requiring access to material/sites normally blocked by university-wide filtering policy in order to undertake academic teaching, learning and/or research. The exemption process for specifics user groups or devices differs to that where or exemptions are being made for the university as a whole i.e. category or sub category changes.

Predominately changes requested will be to request access to a specific site rather than changes to the status of categories or sub-categories.

Specific site access for known user groups or devices

The exemption process for specific sites, user groups or devices is simple with written authorisation belonging to the academic or service Heads of Service, not Technology Services, although a cyber-security threat analysis will be undertaken as a pre-caution prior to any white listing. The IT Service Desk should always be the first point of contact for exemptions of websites for specific users/groups where the written authorisation and justification will be logged for audit purposes.

The university’s technical cyber security and development teams on occasion require exemption from filtering. All requests for unilateral exemption is to be looked for in writing from the Head of Technology Services, or in absence, Head of Information Systems, and logged for audit purposes via the Incident and Request management

University wide Category/Sub-Category changes

Where university-wide changes to filtering policy categories and sub-category are proposed (affecting staff, student or EduRoam/Guest policies), then a short, formal paper should created and submitted to the ***Business Assurance Board*** for approval. For example, this may be for the changing of the Gambling sub-category, currently blocked, to allowed. Any approval should subsequently be passed to the IT Service Desk for category change including the logging of the request for audit purposes via the Incident and Request management system.

On occasion, the university’s filtering service produces false positives; blocking a website that should, in alignment to university policy, be allowed. The IT Service Desk should be alerted in such circumstances and a local assessment carried out (with a cyber-security threat analysis), prior to white-listing. Where a false positive has been determined, with IT team leader acceptance, the website can be white-listed with action logged for audit purposes via the Incident and Request management system.

4. Logging

All user internet activity is securely logged with attempts to access sites (both blocked and allowed) recorded. Activity usage is retained as long as required to support incident management processes.