UNIVERSITY OF SUSSEX

CONTENT FILTERING POLICY (ISP017)

1. OVERVIEW AND PURPOSE

1.1. This policy sets out the principles for support of teaching, research and business activities of University of Sussex whilst protecting users, networks and computers from hostile or unwanted network traffic and illegal or potentially harmful content.

1.2. The University will make use of Internet filtering as part of its approach to managing risks and ensuring safe internet use. There is always a balance between academic freedom and the safety of University people and assets, and this policy identifies where controls may be applied.

Why Content is Filtered?

1.3. Websites may be blocked, or access challenged (giving the user a choice) in accordance with the following:

1.3.1. To support University Policies such as the Acceptable Use Policy.

1.3.2. To support the policies of 3rd parties involved in providing IT Services to the University, such as the JISC Acceptable Use Policy

1.3.3. To support legal or statutory obligations, protect University assets and protect the reputation of the institution

1.3.4. To support the wellbeing of our staff and students by preventing unintended access to unwanted, harmful or illegal materials

Which Content is Filtered?

1.4. Generally, content is not filtered unless it has been deemed to be of some concern. Websites URLs for filtering are grouped under specific categories (e.g. Malware, News, Copyright Infringement, Social Media) to make them easier to manage. By default, these categories are provided by the supplier of the University firewalls and will not normally be maintained by IT Services.

1.5. The University firewalls can either Block Access to a website entirely or can issue a Challenge or warning that requires the user to actively respond.

1.6. **Blocked Access** will inform the user that they cannot access the site and allow them to return to a previous safe location.

1.7. **Challenged Access** will inform the user that they are trying to access a site that is not regarded as safe and give them the choice of continuing or returning to a previous safe location.

1.8. The objectives of this policy are:

1.8.1. To describe how and why the University of Sussex implements content filtering.

1.8.2. To describe what content is blocked and how legitimate requests for access can be made.

2. SCOPE

2.1. This policy applies to all communications carried between the University's networks and the Internet, including web browsing, instant messaging, file transfer and sharing, social media and other standard or proprietary protocols.

3. RESPONSIBILITIES

3.1. University Senior Information Risk Owner (SIRO)

3.1.1. SIRO is overall responsible for the review and approval of this policy.

3.1.2. Periodically review the risks associated with internet content filtering and ensure that appropriate mitigations are in place.

3.2. Director of IT Services

3.2.1. Overall accountability of the implementation of this policy.

3.2.2. Ensure that the duties associated with this policy are resourced and carried out appropriately.

3.2.3. Periodically review the risks associated with internet content filtering and ensure that appropriate mitigations are in place.

3.3. Head of Technical Operations

3.3.1. Ensure that the operational tasks associated with this policy are resourced and carried out appropriately.

3.3.2. Ensure that technical services to apply the filtering are in place and functional.

3.3.3. Ensure that appropriate tools and procedures are in place to enable modifications to the content filtering to be made when required.

3.4. Cyber Security Manager

3.4.1. Ensure that this policy is reviewed and updated periodically or as required.

3.4.2. Ensure that the categories and type of blocking implemented are in line with the requirements of the University.

3.4.3. Ensure that that this policy is aligned with other Cyber and Information Security Policies.

3.5. IT Services Network Team

3.5.1. Implement or revoke firewall content filtering tasks as required and in line with agreement Service Level Agreements.

3.5.2. Correct any technical errors or mis-categorisations in line with Service Level Agreements.

3.5.3. Ensure that any issues arising that need escalation are appropriately handled.

3.6. University Officers, Heads of Schools (and the Dean of BSMS), Directors of Professional Services Divisions and Section Heads

3.6.1. Ensure that all information in their area is protected in conformance with this policy.

3.6.2. Make people in their area of responsibility aware of this policy.

3.7. Researchers and Assistants

3.7.1. Ensure that internet access required for the relevant field of research is available in advance of carrying out research activities.

3.7.2. Ensure that where additional access to blocked sites is required for legitimate research purposes, that the correct process is followed to have access ethically and safely provided.

3.8. Any Users of the University Networks

3.8.1. Follow this policy and associated processes and not make any attempt to circumvent content filtering controls at any time.

3.8.2. Ensure that access for research, study or business activity is available in advance of needing it.

3.8.3. Ensure that any mis-categorised sites are raised through IT Services Help Desk.

3.8.4. Report any Information Security incidents or risks to the Director of IT Services via an appropriate channel.

4. POLICY

4.1. It is the policy of the University of Sussex that all communications will be appropriate secured so as to protect the individuals, assets and the institute from hostile or unwanted network traffic and illegal or potentially harmful content.

4.2. Content Filtering will be applied in support of the University's legal and statutory compliance including, but not restricted to:

4.2.1. Data Protection Act 1998

4.2.2. Copyright Act 1988

4.2.3. Computer Misuse Act 1990

4.2.4. Protection of Children Act 1978[1]

4.2.5. Sexual Offences Act 2003

4.2.6. Criminal Justice and Immigration Act 2008

4.2.7. Counter Terrorism and Security Act 2015

[1] *– The main Sussex network and Eduroam are managed for over-18s and is not child-safe. The guest wi-fi networks should be used to provide safe internet access.*

4.3. Content Filtering will be applied to ensure care towards staff, students and other users of University IT facilities, including restricting access to material known to be used in the radicalisation of individuals into terrorism.

4.4. Content Filtering will be applied to mitigate information and IT security risks posed by computer viruses, malicious software, spam e-mail, phishing, cyber-crime, copyright infringement and illegal file-sharing by preventing access to sites associated with these risks.

4.5. Legitimate academic freedom of access to information in support of research, study or personal development is acknowledged as essential to the operation of the University. The University will provide and maintain a process to enable legitimate requests for exemption to content filtering to be considered and actioned. Access for individuals to blocked sites for legitimate research can be granted by making an application via the research ethics approval processes.

4.6. The University will maintain and publish a list of categories of website that are subject to content filtering.

4.7. Internet filtering log data will be managed in accordance with the University Institutional Access Policy. Trends and activity reports will be maintained as part of monitoring the effectiveness of this policy.

4.8. The Director of IT Services, or nominated deputy, may immediately and without notice temporarily block any site or connection to protect the University IT facilities and its users from cyber threats such as computer viruses, malicious software (malware), spam e-mail, phishing, cyber-crime or Denial of Service (DoS) which are highly dynamic and volatile in nature. Sites blocked temporarily will be reviewed and considered for permanent blocking.

4.9. Any user may request that a site be re-categorised by the suppliers of the University firewalls. Incorrectly categorised sites are normally amended within 24 hours; however, the University can provide a local classification in urgent circumstances or in the event that the supplier will not re-categorise specific content.

5. LEGISLATION AND GOOD PRACTICE

Review / Contacts / References	
Policy title:	CONTENT FILTERING POLICY (ISP017)
Date approved:	25/02/2020
Approving body:	General Counsel, Governance and Compliance

UNIVERSITY OF SUSSEX

IT Services

Last review date:	New policy
Revision history:	0.3
Next review date:	12 months from approval date
Related internal policies, procedures, guidance:	http://www.sussex.ac.uk/infosec/policies
Policy owner:	*Senior Information Risk Officer (SIRO)*
Lead contact / author:	*Pete Collier, Assistant Director, Strategy and Architecture*

SUPPORTING DOCUMENTS

Data Protection policy and guidance - http://www.sussex.ac.uk/ogs/policies/information/dpa/dataprotectionpolicy

Knowledge and Research Exchange policies - http://www.sussex.ac.uk/staff/research/rqi/rqi_information_and_support/rqi_strategy_policy/research-policies

UNIVERSITY OF SUSSEX

IT Services

Appendix One – Categories

When a web site category is accessed one of the following will apply:

Allow —Allow the user to access the web site.

Alert —Allow the user to access the web site and add an alert to the log files.

Report – Allow the user to access the web site, add an alert to the log files, and produce a report for review.

Block —Block access to the web site and add an alert to the log files.

Challenge —Allow the user to access the page by clicking Continue on a warning page. An alert will be added to the log files, and a report produced for review.

Category	**Student own device**	**Staff own device**	**Campus registered device**	**Visitor on eduroam**	**Approved by** (Committee/Role)
Block (Local)	Block	Block	Block	Block	CISO
Command and Control	Challenge	Challenge	Challenge	Challenge	CISO
Copyright Infringement	Alert	Alert	Alert	Alert	SIRO
Crypto-currency	Challenge	Challenge	Challenge	Challenge	SIRO
Dynamic DNS	Alert	Alert	Alert	Alert	CISO
Extremism	Report	Report	Report	Report	SIRO
Grayware	Challenge	Challenge	Challenge	Challenge	CISO
Hacking	Alert	Alert	Alert	Alert	CISO
Malware	Challenge	Challenge	Challenge	Challenge	CISO
Parked	Alert	Alert	Alert	Alert	CISO
Peer-to-Peer*	Alert	Alert	Alert	Alert	SIRO
Phishing	Challenge	Challenge	Challenge	Challenge	SIRO
Phishing (Local)	Challenge	Challenge	Challenge	Challenge	SIRO
Proxy Avoidance and Anonymizers	Alert	Alert	Alert	Alert	SIRO
Questionable	Alert	Alert	Alert	Alert	SIRO
Unknown	Alert	Alert	Alert	Alert	SIRO

**-Peer-to-Peer traffic may be subject to data rate controls during certain hours*

UNIVERSITY OF SUSSEX

IT Services

A complete list of URL categories can be found at https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000Cm5hCAC

Guest Wi-Fi at Sussex is provided by third party companies:

- O2 Wi-Fi https://news.o2.co.uk/2013/09/26/o2-wifi-and-content-filtering/
- Wi-Fi Spark (ACCA only) https://www.wifispark.com/support

This section last updated: March 2020