

# Northumbria University

## Website Whitelisting

### Procedure



Pilot for Blocking 'Hate & Racism' and 'Illegal' Categories

## 1. Pilot

The intent is to block the 'Hate & Racism' and 'Illegal' categories on the University web filter in order to ascertain the number of 'Whitelisting' requests that may be raised in relation to blocking these two groups. This will be in addition to the blocked categories already in place (see below), the current request rate based on the below categories is approx. 1 to 2 requests per week.

- Adult and Pornography
- Bot Nets
- Cheating
- Hacking
- Malware Sites
- Peer to peer
- Phishing and other Frauds
- Proxy Avoid and Anonymisers
- Spyware and Adware

### Proposed Pilot Duration

6 months

### Prerequisites

Prior to commencing the pilot, the following may need to be taken into consideration:

1. The link from the 'Block Page' which appears when a user attempts to access a website currently blocked by the University web filter) requires amending (see Appendix 2). The current Block Page points to an acceptable use statement and may need to be orientated towards the Whitelisting procedure.
2. The Block Page allows the user to click a link generating an email pop up (see Appendix 3), currently the email is blank however this can be 'templated' to assist ascertaining the reason is legitimate and for bona fide University educational or professional purposes, the email should contain:
  - a. Website details (for what they are trying to access)
  - b. Reason for request (bona fide University business or educational reasons)
  - c. Requesters details
    - i. Name
    - ii. Department / Faculty
    - iii. Course

## 2. Policy Insert

The following has now been inserted in to the new, revised IT Security Policy that went before university Executive on 4th Oct 2016:


*The University can exercise its right to use firewall and web filtering technologies to prevent access to undesirable web sites, including in response to the Prevent Duty for Higher Education which requires Relevant Higher Education Bodies, including Northumbria, to consider the use of web filtering in order to deny University users access to extremism-related materials. The current Content Classification System (CCS) through the external web filter provider allows for the application of automatic site blocking by a range of categories i.e. 'Adult', 'Hacking', 'Racism', the list of which is maintained by the web filtering software supplier, not Northumbria University. In the interests of academic freedom, and for bona fide research, teaching and learning purposes, it is recognised that staff and students may require access to sites which are currently blocked based on the criteria of the filtering services. The University has a 'whitelisting' procedure which is detailed in its Acceptable Use Policy. The whitelisting procedure enables staff and students with bona fide requests for access to be granted access through the IT Security Manager to websites and online material which have been blocked through the filtering technologies in force.*

## 3. Proposed Whitelisting Procedure (see Appendix 1 for Flow Diagram)

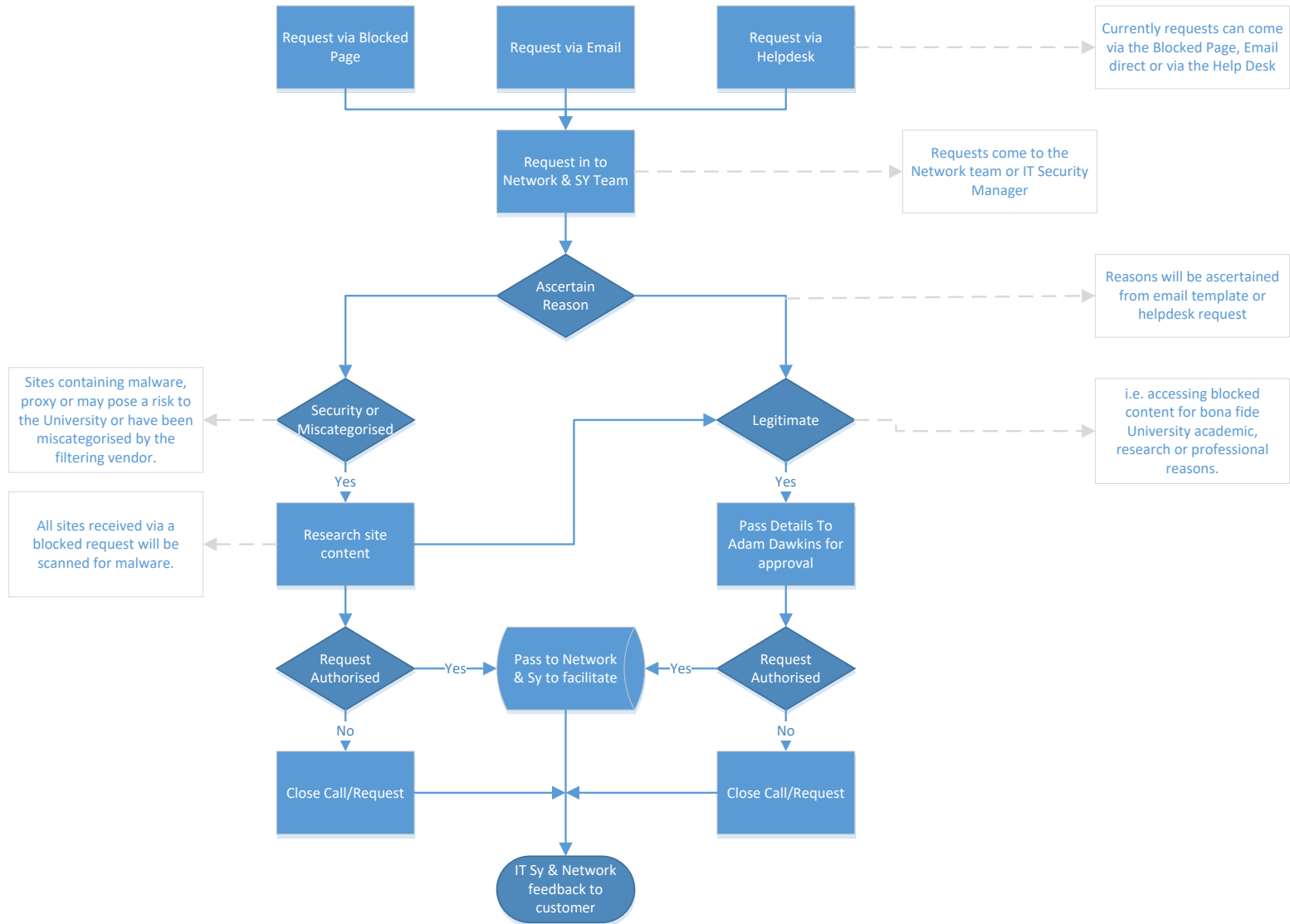
- The request can be raised to the University Network team or IT Security Manager via three channels, the 'Blocked Page', this will be presented on attempting to access a blocked website, the University Helpdesk or directly via email.
- All blocked page requests will be security checked for Malware or the case it may have been miscategorised by the web filter vendor.
- If the website is considered to be unsafe and may cause harm to the University network the request will be declined and details passed to the requester explaining the decision.
- If the website is free from Malware and categorised correctly the details of the request (ascertained either by the Blocked Page generated email template, helpdesk call or direct email, which may require a call back to the requester) will be passed to the University Head of Governance for review. The Head of Governance will pass his decision to the Network team or IT Security Manager to be facilitated, whether the site is Whitelisted or remains blocked the details of the decision will be passed to the requester.

Note: If the website has been miscategorised, the site can be Whitelisted by the Network team or IT Security Manager while the re-categorisation request is made to the web filtering vendor.

### IT Support - open 24 hours, 365 days a year

Email    [it.helpline@northumbria.ac.uk](mailto:it.helpline@northumbria.ac.uk)  
Phone    0191 227 4242  
Chat      [northumbria.ac.uk/itchat](https://northumbria.ac.uk/itchat)  
    [twitter.com/NorthumbriaIT](https://twitter.com/NorthumbriaIT)

# Appendix 1: Requesting Flow Diagram



## Appendix 2: Current Guidance

### Block Page



**Access Denied**

**You are attempting to access a blocked site.**

If you require access to this web site then please contact the System Administrator using the 'Email Reviewer' link below:  
In the email, please include the url (web address) of the blocked site.

[Email Reviewer](#)

Use of the University Network must comply with IT Services Regulations / Guidelines.  
Click [here](#) to read the guidelines.

### Guidance Page

# IT Regulations and Guidance

## IT Regulations and Guidelines

Follow these guidelines to ensure your use of IT facilities is acceptable:

- Computing facilities are provided for academic study and work purposes
- Limited personal use of these facilities is acceptable as long as it does not interfere with academic study or work, or contravene any University regulations.
- Do not use or attempt to use any systems for which you are not authorised.
- Do not use a workstation which has been logged in by another user without permission.
- Keep your username and password secure, do not share them with others.
- Do not attempt to find out or use anyone else's username and password.
- Do not modify the configuration of your system without authority.
- Access to 'inappropriate sites' on the Internet is blocked automatically, do not attempt to bypass this system or download pornographic, criminal or offensive material.
- Do not install or make use of unlicensed software.
- Do not send emails that are libellous, might bring discredit or embarrassment to the University.
- Be aware that your use of the facilities (i.e. emails, Internet usage) may be monitored.

It is your responsibility to make sure your use is acceptable - please ask for advice if you are unsure. Failure to observe the regulations may result in you being suspended without warning from use of the University's facilities and appropriate disciplinary action being taken.

## JANET Acceptable Use Policy

You should also view the JANET Acceptable Use Policy which can be found at:  
<http://www.ja.net/company/policies/aup.html>

## Our current IT Strategies and Policies

- [Acceptable Use Policy](#)
- [Security Policy](#)

## Search Courses

Or try our [Advanced search](#)

View our [Continuing Professional Development \(CPD\) / Short Courses](#)

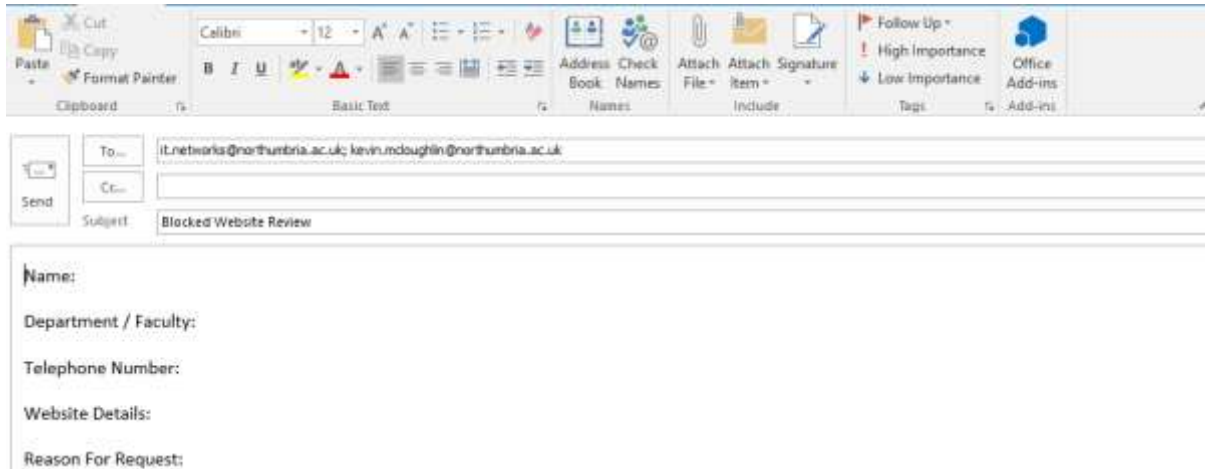
## IT Services

- + [WiFi at Northumbria](#)
- + [Student Email](#)
- + [One Print](#)
- + [IT Support 365](#)
- + [IT Service Availability](#)
- + [IT Access for Visitors](#)
- + [IT Feedback & Customer Care](#)
- + [IT Regulations and Guidance](#)
- + [IT Services Intranet](#)



## Appendix 3: Pre-Formatted Email

Current template:



The image shows a screenshot of an email client interface. At the top is a ribbon with various tabs: Clipboard, Basic Text, Names, Include, Tags, and Add-ins. Below the ribbon are fields for To, Cc, and Subject. The To field contains the email addresses IT.networks@northumbria.ac.uk; kevin.mcloughlin@northumbria.ac.uk. The Subject field contains "Blocked Website Review". Below these fields is a large text area containing a pre-formatted email template with the following labels:

- Name:
- Department / Faculty:
- Telephone Number:
- Website Details:
- Reason For Request: