Hampshire County Council

Hampshire IT

HPSN2 Flexible Web Filtering Admin Guide

Document Version:

Issue Date:

Document Owner: Hampshire IT

This information is available in large print, Braille, audio tape or disk. Please contact the IT Help Desk.

Introduction

This document is a step-by-step guide to using the Client Access page of the HPSN2 Flexible Web Filtering system. It provides users instructions on how to operate and control Client Access.

Table of Contents

1. Initial setup

If your school does not use the Hampshire County Council supplied auto-configuration files then you will need to add some exceptions to your proxy configuration to ensure that you can access the Flexible Web Filtering and Blue Coat Reporter websites.

You will need to add exceptions for:

- ✓ fwfadmin.hiow.gov.uk
- ✓ fwfreporter.hiow.gov.uk

If you do not add these exceptions then you will see a 'connection timed out' message in your web browser as the security on the network will prevent access.

2. Accessing the system

To ensure that each policy is only accessed by the relevant school, a username and password is required which will be sent to the school IT contact.

In order to access the configuration screens a browser needs to be directed to the following:

- ✓ Flexible Web Filtering: http://fwfadmin.hiow.gov.uk
- ✓ Bluecoat Reporter: http://fwfreporter.hiow.gov.uk:8081/
- ✓ You will need to login using the username and password supplied. These are case sensitive.

3. Supported browsers

The following browser versions are supported:

Flexible Web Filtering:

- ✓ Microsoft Internet Explorer 7 and 8
- ✓ Firefox 3 and 4;
- ✓ Safari 4

Bluecoat Reporter:

- ✓ Firefox 3.6.x
- ✓ IE 7 and 8.

4. Logging On and Off

Start Internet Explorer and enter the URL that has been supplied. The service will present a login form requesting a username and password:

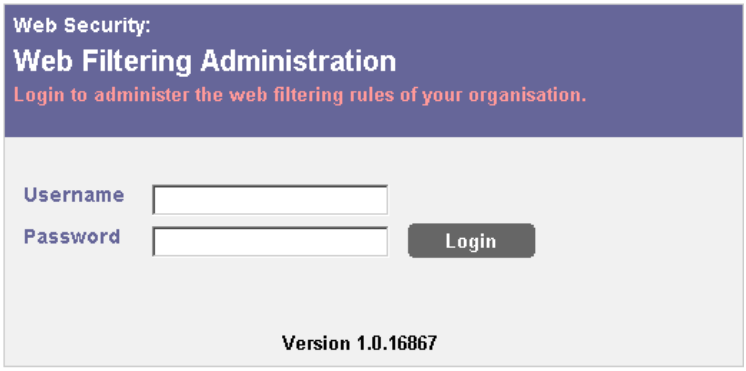

Fig.1 – Login screen

Enter the details as they were supplied and click 'Login'. Once logged in you should be presented with a screen resembling the screenshot below. This screen is referred to as the '**User Interface**' or '**UI**'

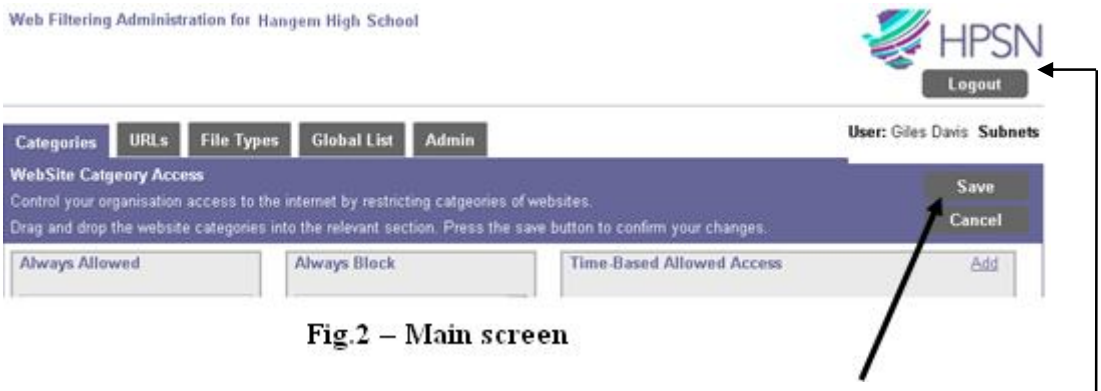

Fig.2 – Main screen

After changing any configuration settings please ensure you **save** your changes. We recommend that you log out immediately afterward saving. The logout button is located in the top right-hand corner below the HPSN2 logo.

5. Reviewing URLs

This function contacts Blue Coat to check in which category a specified URL has been placed.

- ✓ Click the 'Admin' Tab.
- ✓ From the Admin tab, click on Review URL.
- ✓ When presented with the screen below, enter (or paste) the URL that you wish to check
- ✓ Click Check Rating.

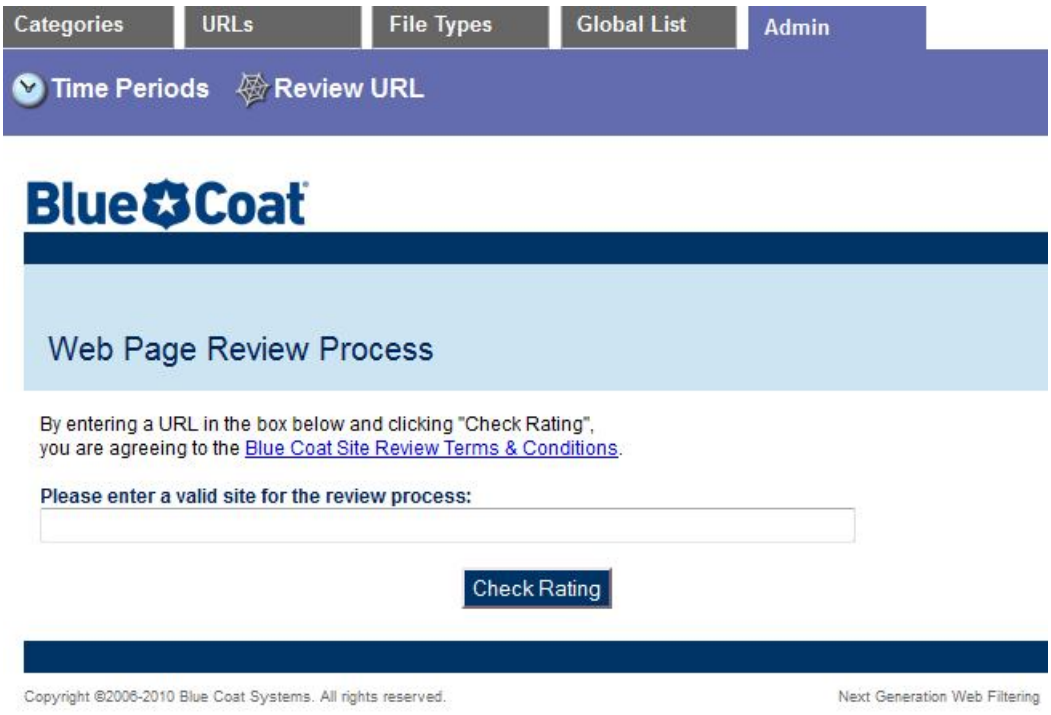

Fig.3 – Web Page Review Process

- ✓ The requested information should now be displayed as below

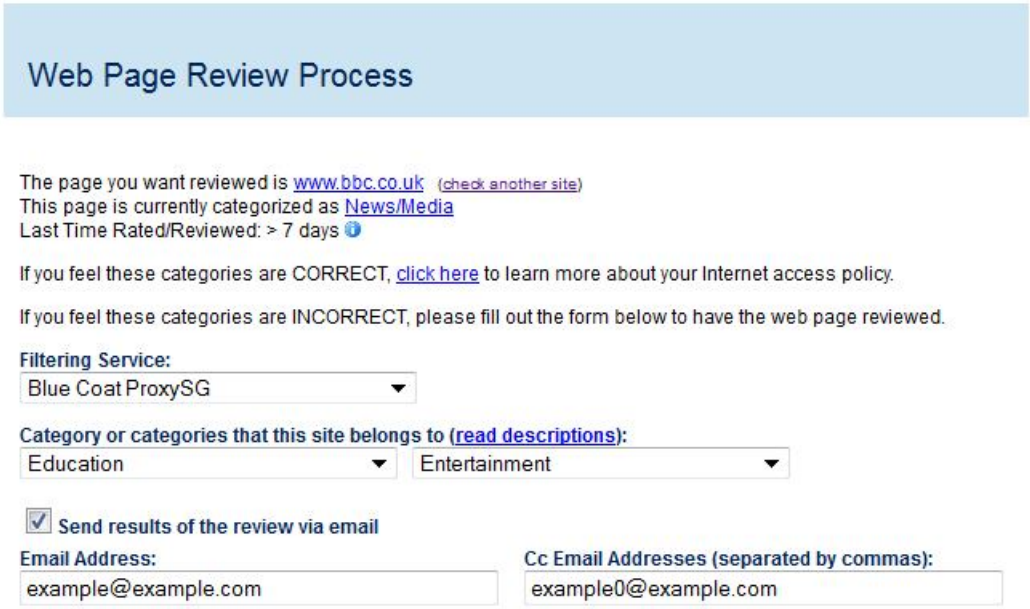

Fig.4 – Re-categorisation Request

If you feel that the URL has been miscategorised, it is possible to complete the form (shown in Fig.4 above) and submit a request for re-categorisation to Blue Coat. **Please note, the categorisation is administered by Blue Coat, and not Hampshire County Council.**

- ✓ Select **Blue Coat** ProxySG as the filtering service
- ✓ Select the category or categories you feel better describes the site.
- ✓ Tick 'Send results of the review by email'.
- ✓ Complete the main email address and list any Cc email addresses separated by commas
- ✓ Once complete click '**Submit for Review'**.

6. Adding New Time Periods

You can create user defined time periods, for example **'Lunch',** which will be associated with your lunch start and end times. These named time periods can then be used for blocking or allowing access to web pages at specific times of the day.

- ✓ Navigate to the Admin tab of the UI.
- ✓ Click 'Time Periods'.
- ✓ Within this window, click on the link labelled 'Add a new Time Period'.
- ✓ The box shown in Fig.5 will appear.
- ✓ Type in a name for the time period.
- ✓ Complete the 'From' and 'To' times using 24 hour clock notation
- ✓ Tick the days appropriate for the time period.
- ✓ **NB** The fields marked with a '*' are required fields and so cannot be left blank. You can abort any changes by clicking **Cancel** at any time prior to **Saving**.

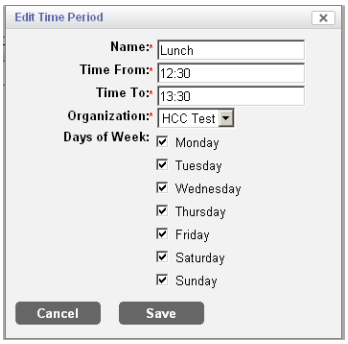

Fig.5 – Creating a new Time Period

A new Time Period will be created and displayed in the UI as shown in Fig.6.

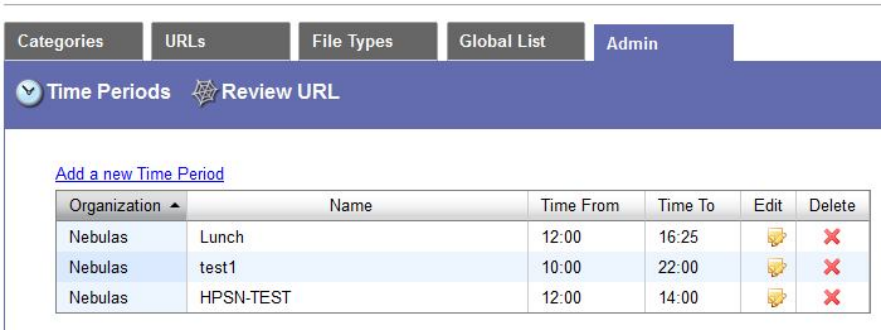

Fig.6 – New Time Period Added

- ✓ To edit a Time Period, click the icon in the Edit column adjacent to the named period.
- ✓ To delete a Time Period click on the icon in the Delete column adjacent to the named period.
- ✓ To see the new time period in the Categories tab you will need to refresh the page.

7. Global List

The global list tab displays the Global Polices applied via HPSN2 Flexible Web Filtering. The output is displayed in a rule-based format. An example is shown in Fig.7.

Fig.7 – Global Rules

- ✓ It is possible to see further information about the rule by clicking on the magnifying glass next to the 'Service' column (circled in Fig.8).

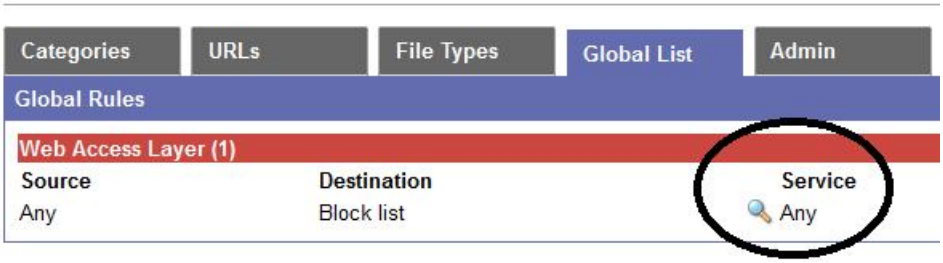

Fig.8– Click to view Further Service Information

8. 'Allow' and 'Block' by File Type

The File Type control tab provides flexible provisioning of 'allow' and 'block' lists by file types. To add or remove file types to either configurable list, the process is essentially the same.

- ✓ Navigate to the **'File Types'** tab.
- ✓ Click '**Add**' on either the '**Allowed'** or '**Blocked'** column as appropriate. (**Fig. 9**)
- ✓ Select the options you require from the window that 'pops up' on the screen (**Fig.10**).
- ✓ Click 'Add'.
- ✓ Repeat this process if required.
- ✓ In order to remove a file type, click on the red 'X' in the corresponding row.
- ✓ Click 'Save' to retain the completed changes.

NB – If you hover the mouse over the file extension type in the list, it will give you a brief description of what the extension pertains to.

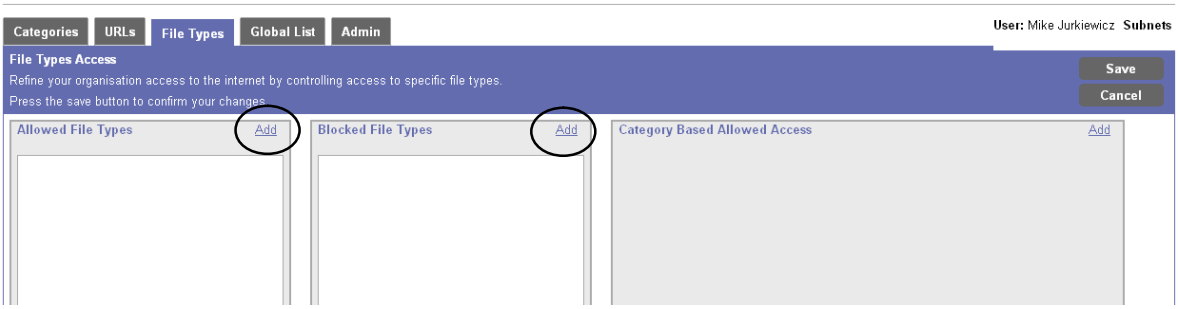

Fig. 9 – File Types

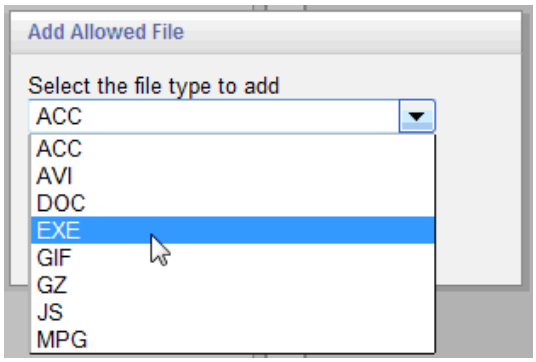

Fig. 10 – File Types pop up

9. Controlling access by URL

In order to create a more granular web filtering policy, it is possible to add specific URLs to this section which will override their categorisations. It's worth noting that you cannot override the global list.

To add or remove URLs to any of the configurable lists, the process is essentially the same.

9.1. To Allow URLs:

- ✓ Navigate to the URLs tab.
- ✓ Click 'Add' in the Window labelled 'Allowed URLs' (Fig.10).
- ✓ In the window that then opens, enter (or paste) the required URL that you wish to allow.
- ✓ Click Add. (You can also choose to review, this will parse the URL to Blue Coat Website review page in a new Browser Window)
- ✓ Click 'Save'.

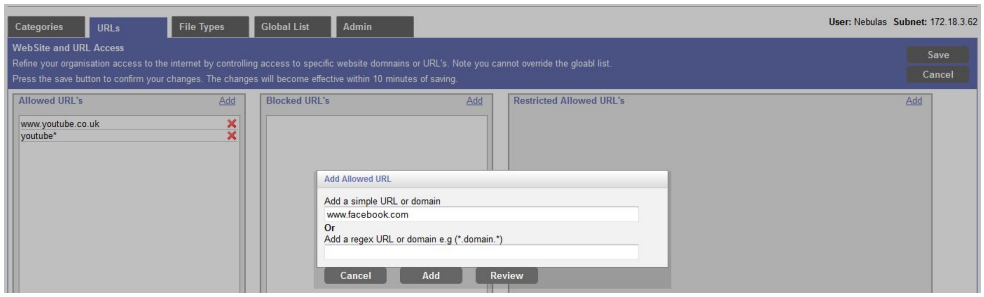

Fig.10 – Adding a URL to Allowed URLs

9.2. To Block Specific URLs:

- ✗ Navigate to the URLs tab.
- ✗ Click 'Add' in the Window labelled 'Blocked URLs'.
- ✗ In the window that then opens, enter (or paste) the required URL or wildcard expression that you wish to block.
- ✗ Click Add. (You can also choose to review; this will parse the URL to Blue Coat Website review page in a new Browser Window).
- ✗ Click 'Save'.

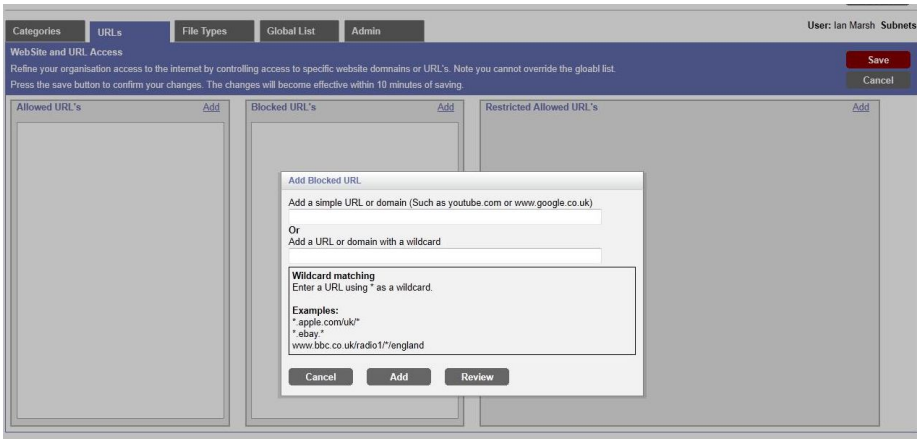

Fig.11 – Adding a URL to the Blocked URLs

If you wish to allow previously restricted URLs so that they're ONLY accessible during certain time periods, it is possible to do so using 'Restricted Allowed URLs'; this is described below.

Restricted Allowed URLs:

- ✓ Navigate to the URLs tab.
- ✓ Click 'Add' in the Window labelled 'Restricted Allowed URLs'.
- ✓ In the window that then opens, enter (or paste) the required URL or wildcard expression that you wish to allow and select a time period (which should have already been created in the admin tab – see previous section labelled 'Add new Time Period' for details).
- ✓ Click Add. (You can also choose to review; this will parse the URL to the Blue Coat Website review page in a new Browser Window).
- ✓ Click 'Save'.

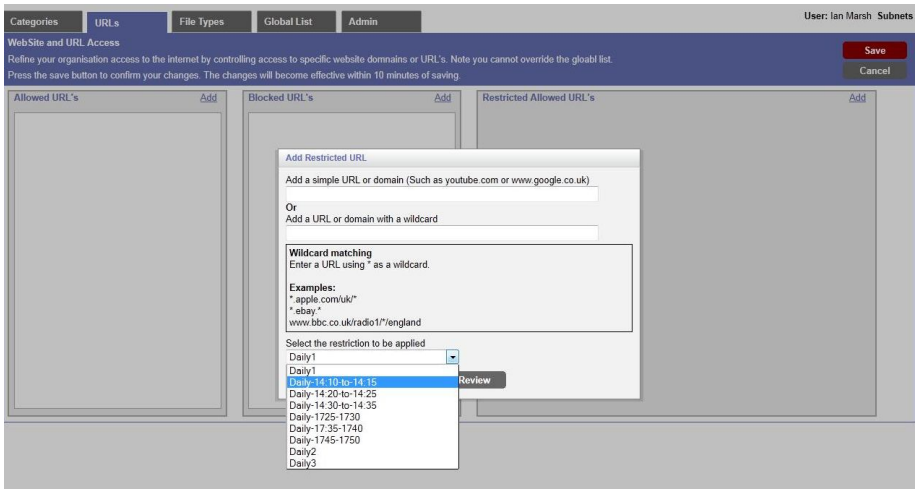

Fig.12 – Adding Restricted Allowed URLs

9.3. Examples of Simple and Wildcard URLs

The following tables list some common sites, domains, sub domains, or wildcard URLs which will need to be added to the administration site to either allow or block the requested site as appropriate. The IT Help Desk receives quite a number of calls from schools wanting to block Google images, for example, as it isn't as obvious as simply blocking or allowing a specific site.

9.3.1. General Websites

Website	URL Type	Filter String
Facebook	Simple	facebook.com fbcdn.net
Twitter	Simple	twitter.com twimg.com
YouTube	Simple	youtube.com ytimg.com
eBay	Simple	ebay.com ebayimg.com ebayinc.com ebayrtm.com ebaystatic.com ebaypartnernetwork.com ebayadvertising.com

9.3.2. Search Engines

Search engine	URL Type	Images	Video
Google	Wildcard	*.google.*/*tbm=isch* *.google.*/image*q=* *.google.*/advanced_image_search*	*.google.*/*tbs=*vid*
Yahoo	Wildcard	*.yahoo.com/*img*?* *.yahoo.com/*image*?*	*video.yahoo.com*
Ask.com	Wildcard	*ask.com/pictures*	*ask.com/video*

10. Categories

The categories section is where most of the web filtering policy will be defined. The policy is controlled using a drag-and-drop interface (see Fig. 13).

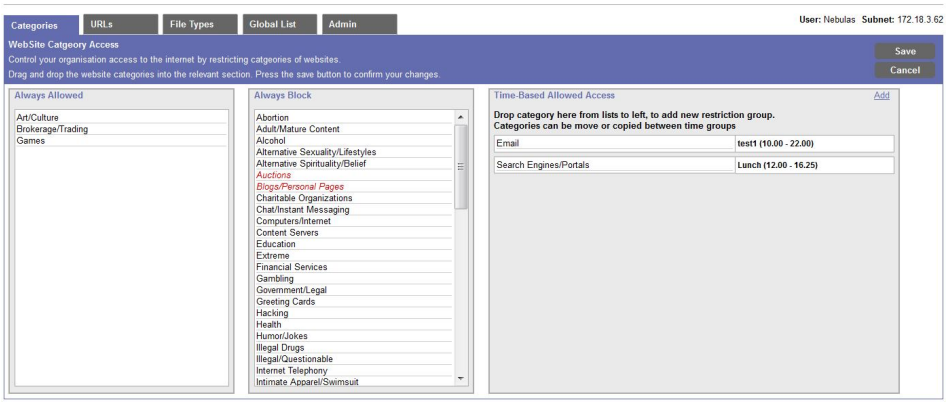

Fig.13 – Category View

10.1. Creating a Web Filtering Policy Using the Category View:

- ✓ Navigate to the Categories tab.
- ✓ Drag all the categories (by holding down the left mouse button on the desired category listing) that you wish to 'Allow' into the 'Always Allowed' Column. See Fig.13.
- ✓ Drag all the categories (by holding down the left mouse button on the desired category listing) that you wish to 'Block' into the 'Always Block' Column. See Fig.13.
- ✓ Click 'Save' when complete.

10.2. Creating a Time-Based Allowed Access Policy:

- ✓ Navigate to the Categories tab.
- ✓ Click 'Add' within the 'Time-Based Allowed Access' window.
- ✓ Select an appropriate time period and click 'Add'.
- ✓ Drag the required categories (by holding down the left mouse button on the desired category listing) that you wish to 'Allow' during that time period into the Column. See Fig.14.
- ✓ Click 'Save' when complete.

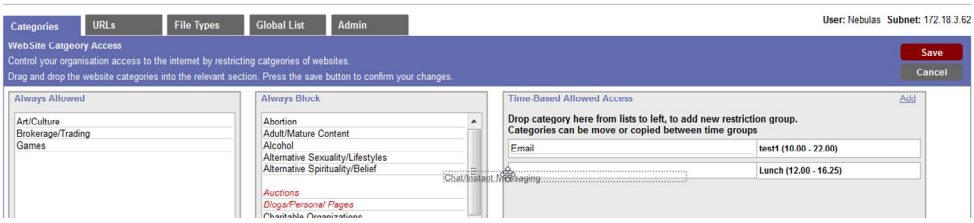

Fig.14 – Time-based Allowed Access (Dragging-and-Dropping)

11. HSPN2 Flexible Web Filtering school responsibilities

By using HPSN2 Flexible Web Filtering it is important that the school management team understands and takes responsibility for the implications and consequences of this action. This flexible filtering tool provides the school with the potential to retrieve harmful, unsuitable and illegal websites, and this content could then be accessed by pupils and staff. The Senior Leadership Team must ensure that the school internet usage policy complies with Hampshire IT standards and that the filters in place restrict access to inappropriate material.

Current E-Safety guidelines can be found at:

http://www.hants.gov.uk/esafety

The DfES recommend that the following categories should not be available to any school:

- ✗ Pornographic, adult, tasteless or offensive material
- ✗ Violence (including weapons and bombs)
- ✗ Racist, extremist and hate material
- ✗ Illegal drug taking and promotion
- ✗ Criminal skills, proxy avoidance and software piracy

These are blocked centrally and cannot be unblocked.

By accepting this disclaimer and using the HSPN2 Flexible Web Filtering service the school agrees that it:

- ✓ Is wholly responsible for the configuration of the filtering profile that is provided.
- ✓ Acknowledges the potential ability to provide pupils and staff with an unfiltered internet feed.
- ✓ Accepts responsibility for, and the consequences of, any inappropriate content that is accessed, uploaded, downloaded to, or posted from the school's network.
- ✓ Will assist Hampshire County Council and/or the police in any investigation that arises from the school's use of the internet through the HPSN2 Flexible Web Filtering solution, and any action that has been taken using the solution.

If you come across a site which you think should be allowed or blocked for all schools (i.e. added to the global list) then please contact Hampshire IT as normal to request this **even if you are on Flexible Web Filtering**.