Carniny Primary School

Internet Filtering Policy

October 2018

Internet Filtering Policy

The contents of this policy pay close attention to the following DE Circulars:

- DE Circular 2011/22: Internet Safety
- DE Circular 2007/01: Acceptable Use of the Internet and Digital Technologies in Schools.

Copies of the above can be accessed online at www.deni.gov.uk; hard copies will also be stored with this policy document.

Everyone at Carniny Primary School takes internet use and the associated safety of our pupils extremely seriously.

It is important to note, however, that any filtering service, no matter how thorough, can never be comprehensive and it is essential both that schools have a clearly understood policy on acceptable use for all users and that adequate supervision is maintained.

If at any time school staff or pupils find themselves able to access internet sites from within school which they think should be blocked, they should advise the school Principal (or, in his absence, the ICT Leader). The Principal should then report the matter to **the C2k Helpdesk / iTeach** who will implement agreed procedures for handling such issues.

Depending on the nature of the issue, these procedures may require C2k to report to the Department. All actions should be taken immediately.

Two Systems

In Carniny Primary School we use two systems for internet access:

1. DE provided C2K provision;
2. Non-DE/C2K provided 'BT Infinity' fibre optic broadband.

DE provided C2K provision

C2k provides an effective filtering system, as a result of which the following
categories of websites are not, by default, available to schools: -

- **Adult**: content containing sexually explicit images, video or text, the depiction of actual or realistic sexual activity;
- **Violence**: content containing graphically violent images, video or text;
- **Hate Material**: content which promotes violence or attack on individuals or institutions on the basis of religious, racial or gender grounds;
- **Illegal drug taking and the promotion of illegal drug use**: content relating to the use or promotion of illegal drugs or misuse of prescription drugs;
- **Criminal skill/activity**: content relating to the promotion of criminal and other activities;
- **Gambling**: content relating to the use of online gambling websites or information relating to the promotion of gambling and gambling advice.

C2k defines three types of access:

- GREEN – accessible to all users in schools;
- AMBER – accessible to schools' selected groups of users (can be changed by the C2K School Manager within Post-primary and Special schools only);
- RED – not accessible to any user.

C2K filtering is managed at departmental level and is **not the responsibility of the school**.

Non-DE/C2K Provided 'BT Infinity'

Departmental Circular 2011/22 states that if a school sets up its own school network, separate from the C2k managed service, with its own internet connection and Internet Service Provider (ISP), it is the school's responsibility to ensure that the filtering system provided is of an appropriate standard to ensure the safety of its pupils.

Whether a school has an agreement with its ISP for a filtering system, or has the expertise to install and maintain its own filtering system, it is vital that it has a filtering policy in place. In drawing up such a policy, a school should ensure that the following are taken into account (this list is not exhaustive).

To that end in Carniny Primary School we enlisted 'iTeach' (independent educational ICT company) to oversee the installation of our BT Infinity and associated filtering system. We have now joined the long list of schools who have 'paired-up' to work with iTeach on a long term basis.

iTeach Internet Filtering

Summary
The schools wifi and infrastructure has been installed and is maintained with an active, monitored filter system to satisfy both the needs of child protection/inappropriate content whilst ensuring that it serves to support teaching and learning.

This document details all aspects of the filtering policy and systems for 'the network', also referred to here as 'classnet'

Access to network
Access to the network is provided through password authentication using WPA. This key is not available to any staff aside from the school SLT. Access is therefore governed by unique device registration and pre approval by authorised staff only. No devices can join the network without this approval and authentication.

Hardware and general service provision
The following has been installed and configured in school to ensure only appropriate content is available to all users:

1. A hardware firewall filter is installed which intercepts all Internet traffic leaving and entering the school network and this cannot be circumvented. This firewall appliance is configured for the Globalview Internet filtering service, powered by industry giant Cyren. This service is a professional, commercial category based web filtering solution in use by over 120k schools worldwide. It uses a category based system to group web sites in addition to keyword, IP and specific white and blacklist control. School licenses are purchased on a fixed three year term to ensure continuity of service and the individual firewall is monitored 24/7 with instant notification of any concerns.

2. In addition, IP and URL black and white listing is supported locally which ensures any content that is flagged as non desirable on the network, can be disabled immediately

3. Full access logs are maintained for all traffic and all attempts at access of inappropriate content.

Specifics of filtering service

This filtration service uses a category based system to decide if a website is viewable from all Internet connected devices. The primary Categories include:

- Child Protection (including violence, porn, weapons etc)
- Leisure (entertainment, travel, sports)
- Business
- Chatting (internet chatting and instant messaging services)
- Computer & Internet Services (social networking, streaming, spam sites)
- Other (image sharing, dating and person, compromised, inc uncategorised)

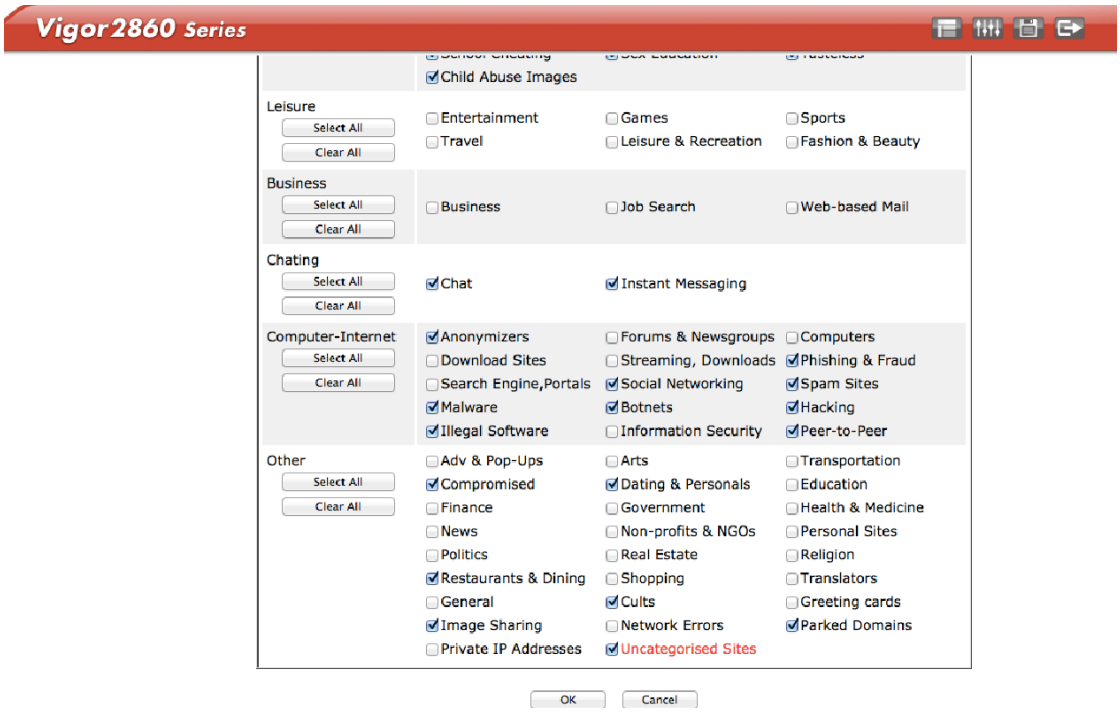
If a website falls into a category that is not deemed acceptable for use in the classroom. The user will be subject to viewing an "unsuitable" notification on the web browser and this activity logged to user and device level. Cyren independently search the Internet using their tools to

select what category is assigned to any available website. This is then matched to the live filtering within the school.

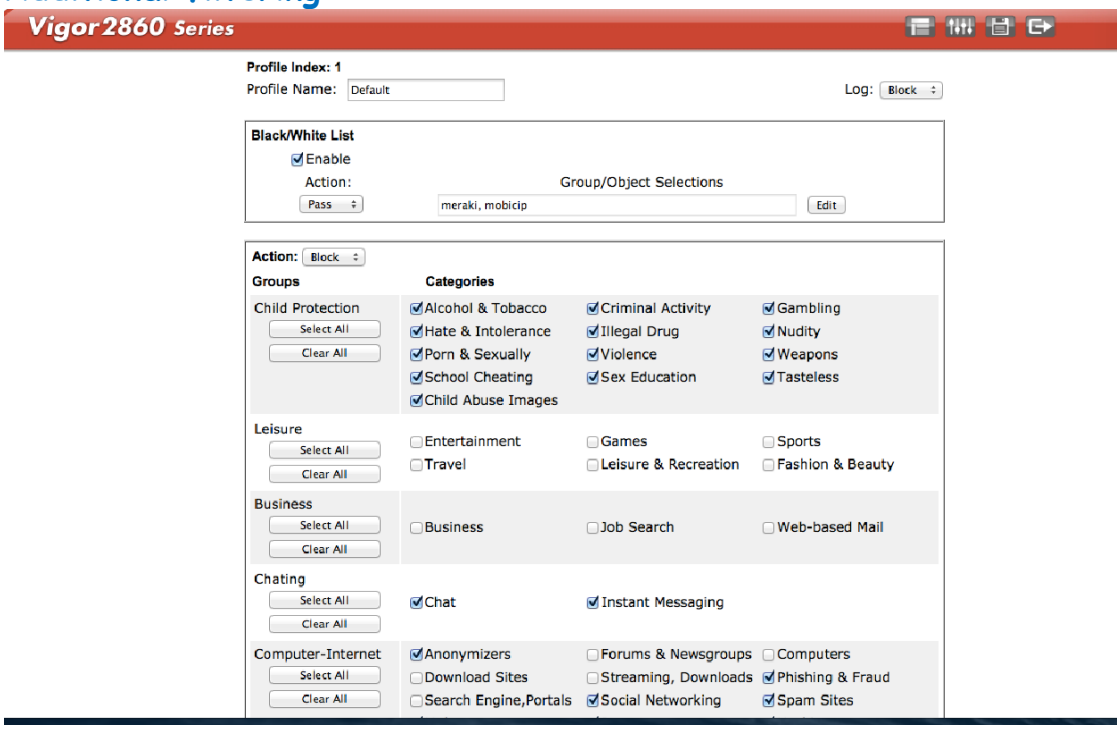
A website's category can be manually checked and identified by using their free, up to date database tool:

http://www.cyren.com/url-category-check.html

The default categories selected are as follows:



Additional filtering



To supplement category based filtering, the school maintains a rolling list of websites requested by teaching staff, checked and approved to be exempt from category filtering and this is available in school. This list is maintained by the ICT technician and relevant eSafety coordinator. Websites are added to a specific blocking list where required.

School Procedures

The school has a mechanism should a website be found to be uncategorised, and can request a category to be allocated from within the URL category tool.

Individual websites and iOS apps can be permitted through the filtering system on a site per site basis using a system called White Listing. This is particularly useful when blocking such apps as Twitter, Facebook and Tumblr that operate within an 'App' environment.

Additional filtering for mobile devices

Standard browsers are removed (e.g. Safari) and are replaced by a secure browser which adds a second filtering level per device. This is controlled on age based settings and is secondary to the firewall filtering. No pupil can access an unfiltered browser.

All devices are supervised which enables Internet access control at OS level, which offers a final layer of filtering based in content groups and discrete Internet addresses.

Further Notes

- Filtering has been checked by two senior staff within Dept Guidelines.
- Two members of staff have been trained in filter use in order to react with speed for any system issue.
- The network is supported on demand from an external agency (iTeach)
- The schools eSafety Policy has been changed to match these changes and systems.

This policy was compiled in October 2018 and is subject to review and updating as required.