The Nicholas Hamond Academy
Internet Filtering Policy

Date of introduction: December 2016

Date of Review: December 2017

Signed …… Acting Principal

Date ……

Signed …….. Chair of Governors

Date ……

Member of staff responsible: Mr. S. Baxter

1.0 Purpose

The purpose of this policy is to define standards for systems that monitor and limit web use from any host within The Nicholas Hamond Academy's network. These standards are designed to ensure everyone uses the Internet in a safe and responsible manner, and ensure that individual web use can be monitored or researched during an incident.

2.0 Scope

This policy applies to all The Nicholas Hamond Academy staff, students' contractors, vendors and agents with an academy-owned or personally-owned computer or other device connected to the academy network. This policy applies to all end user initiated communications between The Nicholas Hamond Academy's network and the Internet, including web browsing, instant messaging, file transfer, file sharing, and other standard and proprietary protocols. Server to Server communications, such as SMTP traffic, backups, automated data transfers or database communications are excluded from this policy.

3.0 Policy

3.1 Web Site Monitoring

IT Support Services shall monitor Internet use from all computers and devices connected to the academy network. For all traffic the monitoring system must record the source IP Address, the date, the time, the protocol, and the destination site or server. Where possible, the system will record the User ID of the person or account initiating the traffic. Internet Use records are preserved for 365 days.

3.2 Internet Use Filtering System

IT Support Services shall block access to Internet websites and protocols that are deemed inappropriate for The Nicholas Hamond Academy's working environment using the Smoothwall filtering system. Smoothwall is a member of the Internet Watch Foundation and utilises both the IWF CAIC list of URLs and the Police assessed list of unlawful terrorist content produced by the Home Office.

The filtering system comes with a number of standard categories as well as the ability to add custom URL's as required. These categories are updated on an hourly basis automatically.

The following protocols and categories of websites are blocked:

- Chat & Instant Messaging
- Gambling
- Peer to Peer File Sharing
- Web Based Email
- Adult Entertainers
- Adult Sites
- Criminal Activity
- Gore
- Restricted to Adults
- Web Proxies
- Dating Sites
- Social Networking
- Advertising
- Child Abuse
- Drugs
- Intolerance
- Pirate & Copyright Infringement
- Pornography

- Online Games
- Hacking
- Malware & Phishing
- Weapons
- Terrorism
- Violence
- Sexuality Sites
- Payday Loans

This is not an exhaustive list and may change as technology develops, some websites may be listed in more than one category.

3.3 Internet Use Filtering Rule Changes

The IT Manager shall periodically review and make any changes to web and protocol filtering rules either in response to e-safety incidents or Internet developments. Changes to web and protocol filtering rules will be recorded in the Internet Use Monitoring and Filtering Policy.

3.4 Internet Use Filtering Exceptions

If a site is miscategorised, staff may request the site be un-blocked by submitting a ticket to the IT Support Services help desk. A member of the IT Support Services will review the request and un-block the site if deemed to be miscategorised.

4.0 Enforcement

The IT Manager will periodically review Internet use monitoring and filtering systems and processes to ensure they are in compliance with this policy.

5.0 Definitions

Internet Filtering – Using technology that monitors each instance of communication between devices on the corporate network and the Internet and blocks traffic that matches specific rules.

User ID – User Name or other identifier used when an associate logs into the academy network.

IP Address – Unique network address assigned to each device to allow it to communicate with other devices on the network or Internet.

SMTP – Simple Mail Transfer Protocol. The Internet Protocol that facilitates the exchange of mail messages between Internet mail servers.

Peer to Peer File Sharing – Services or protocols such as BitTorrent and Kazaa that allow Internet connected hosts to make files available to or download files from other hosts.

Social Networking Services – Internet sites such as Myspace and Facebook that allow users to post content, chat, and interact in online communities.

SPAM – Unsolicited Internet Email. SPAM sites are websites link to from unsolicited Internet mail messages.

Phishing – attempting to fraudulently acquire sensitive information by masquerading as a trusted entity in an electronic communication.

Hacking – Sites that provide content about breaking or subverting computer security controls.