	Internet Filtering Policy		
Date adopted	June 2018	**Owner**	SBM
Last reviewed		**Review cycle**	2 Years

Purpose

This document sets out the policy for Internet filtering at St Martin's CofE Voluntary Aided Schools. Internet filtering is necessary to block access to those websites that are illegal, or considered to be inappropriate for children, although filtering also blocks access to those sites considered inappropriate for staff.

It is intended that this policy ensures that measures are in place to ensure the safety of children whilst using the Internet at school, and provides guidance for those involved in ensuring that measures are regularly reviewed and tested.

Filtering solution

Internet filtering at St Martin's will comprise three elements:

A commercial Internet filtering package specifically designed for education from Lightspeed Systems

The ability to amend the normal filtering (ie blocking or unblocking) based on a clear procedure involving appropriate authorisation – see para 8

Random checks to ensure that filtering is providing an appropriate level of blocking

These are considered in more detail below.

Lightspeed Systems

New websites are being created continuously all over the World. It is simply not possible for an individual to monitor all new sites and determine which should be allowed or barred, and to whom. A number of commercial companies continuously monitor Internet sites and provide filtering packages designed to meet the needs of specific types of user. The filtering solution employed at St Martin's is a commercial offering from Lightspeed Systems, which is specifically designed for educational use. Lightspeed are a well established filtering company and have been supporting IT in schools since 1999.

We do not have a direct contractual relationship with Lightspeed, but we subscribe to their services as part of our Internet package which is provided by EAC network Solutions. This is normal practice for smaller educational establishments such as St Martin's.

Appropriate filtering for education

The Department for Education published revised statutory guidance 'Keeping Children Safe in Education' in May 2016 (and active from 5th September 2016) for schools and colleges in England. Amongst the revisions, schools are obligated to "ensure appropriate filters and appropriate monitoring systems are in place. Children should not be able to access harmful or inappropriate material from the school or colleges IT system" however, schools will need to "be careful that "overblocking" does not lead to unreasonable restrictions as to what children can be taught with regards to online teaching and safeguarding."

The UK Safer Internet Centre provides guidance to help education settings (including Early years, schools and FE) and filtering providers comprehend what should be considered as 'appropriate filtering'. It is important to recognise that no filtering systems can be 100% effective and need to be supported with good teaching and learning practice and effective supervision. This guidance can be found at:

https://www.saferinternet.org.uk/advice-centre/teachers-and-professionals/appropriate-filtering-and-monitoring/appropriate-filtering

Extracts from this guidance is given in paras 5 and 6 below.

Illegal online content

In considering filtering providers or systems , The UK Safer Internet Centre states that schools should ensure that access to illegal content is blocked, specifically that the filtering providers:

Are Internet Watch Foundation (IWF) members and block access to illegal Child Abuse Images and Content (CAIC)
Integrate the 'the police assessed list of unlawful terrorist content, produced on behalf of the Home Office'

Lightspeed are IWF members and conform to the above.

Inappropriate online content

Recognising that no filter can guarantee to be 100% effective, the UK Safer Internet Centre states that schools should be satisfied that their filtering system manages the following content (and web search). Discrimination: Promotes the unjust or prejudicial treatment of people on the grounds of race, religion, age, or sex.

Drugs / Substance abuse: displays or promotes the illegal use of drugs or substances

Extremism: promotes terrorism and terrorist ideologies, violence or intolerance

Malware / Hacking: promotes the compromising of systems including anonymous browsing and other filter bypass tools as well as sites hosting malicious content

Pornography: displays sexual acts or explicit images

Piracy and copyright theft: includes illegal provision of copyrighted material

Self Harm: promotes or displays deliberate self harm (including suicide and eating disorders)

Violence: Displays or promotes the use of physical force intended to hurt or kill

The filtering provided by Lightspeed meets these criteria.

Prevent

To assist schools in complying with the Prevent duty guidance of the UK Counter Terrorism and Security Act 2015, Lightspeed Systems has established a violence/extremism category which is populated with a list of web addresses that promote extremism and/or radicalization. The list is supplied to Lightspeed Systems from the Home Office and the category is updated every time the Home Office supplies a list. All information in the list is secure and cannot be accessed.

Filtering system features

The UK Safer Internet Centre additionally recommends that schools should consider that their filtering system meets the following principles. The extent to which our system meets these principles is indicated.

Age appropriate, differentiated filtering – includes the ability to vary filtering strength appropriate to age and role. We can apply filtering to KS1 and KS2 independently.

Control - has the ability and ease of use that allows schools to control the filter themselves to permit or deny access to specific content. All of our filtering is controlled via EAC.

Filtering Policy – the filtering provider publishes a rationale that details their approach to filtering with classification and categorisation as well as over blocking. We do not have sight of Lightspeed's rationale.

Identification - the filtering system should have the ability to identify users. Internet filtering at St Martin's is applied to specific machines, not individual users. We are not able to identify individual users.

Mobile and App content – isn't limited to filtering web traffic and includes the blocking of inappropriate content via mobile and app technologies. Blocking applies to our Wifi network and any guest users of our network.

Multiple language support – the ability for the system to manage relevant languages. Not known.

Network level - filtering should be applied at 'network level' ie, not reliant on any software on user devices. Filtering is applied at Network level.

Reporting mechanism – the ability to report inappropriate content for access or blocking. Not known.

Reports – the system offers clear historical information on the websites visited by your users. Not available as individual users cannot be identified.

Requests to block or unblock specific sites

From time to time staff may wish to have access to sites that are normally blocked by our filter. In such cases we require those requesting access to complete the form shown at Appendix A. They should clearly state the site(s) to which access is required, who should have access, and why it is required. The form will then be submitted to the Executive Leadership Team (ELT) who will consider the request and approve or reject it. Approved requests will be passed to the IT support team who will forward the request to EAC to implement. The IT support team will maintain a list of all approved requests. The list will be reviewed by the IT support team/ELT on an annual basis.

A similar process will apply if staff request that access to a specific site is blocked.

Ad hoc checking

The IT support team will conduct random (at least termly) checks to ensure that Internet filtering is being applied appropriately. It is recognised that such testing cannot be exhaustive, but will simply check that some of the more obvious inappropriate sites are blocked. A record of all testing undertaken will be maintained by the IT support team, both to confirm that this element of our filtering policy is being carried out, and also to protect those who are carrying out the checks from potential allegations of computer misuse.

Appendix A

Request to Amend Internet Filtering

Title	
Please unblock/block (delete as appropriate) the following sites (list all urls):	
Reason	
Please apply to the following groups:	Tick all that apply
Office staff	
Teaching staff	
KS1 pupils	
KS2 pupils	
Other (please specify)	
Requested by:	
Date requested:	

ELT decision	Approved/not approved
Authorised by	
Date of Decision	

Date referred to EAC	
Date filtering implemented	