Becky Heaton
February 2023

Filtering at Surrey Teaching Centre

Surrey Teaching Centre use RM Education as our broadband provider. RM SafetyNet has a 'core rules' list comprising over 1.6 million known URLs. This includes all of the illegal sites on the Internet Watch Foundation and 'Prevent' ('police assessed list of unlawful terrorist content, produced on behalf of the Home Office') list, alongside 13 other categories of 'inappropriate' content.

Satisfying the latest DfE guidelines:

RM SafetyNet satisfies all the filtering requirements, as set out in the latest 'Keeping Children Safe in Education' DfE Guidance Document, the Prevent Duty and Ofsted's Common Inspection Framework. To list the minimum requirements now expected of schools (as set out in 'Keeping Children Safe'),

RM SafetyNet will:

- Block Access to illegal content (i.e. the Internet Watch Foundation and 'Prevent' filter lists)
- Prevent access to inappropriate content (i.e. anything categorised as Discrimination, Drugs/Substance abuse, Extremism, Malware/Hacking, Pornography, Piracy and copyright theft, Self-Harm, Violence)

In addition to the features required as part of Keeping Children Safe, RM SafetyNet will also intercept HTTPs traffic, enable guest users to receive automatic filtering via a transparent proxy and provide a reporting feature that enables the School's Designated Safeguarding Lead to create and study activity reports at multiple levels, for example individuals and individual sites.

We are confident that our filtering providers:

- Are IWF members and block access to illegal Child Sexual Abuse Material (CSAM)
- Integrate the 'the police assessed list of unlawful terrorist content, produced on behalf of the Home Office'

Surrey Teaching Centre Leadership and Management Committee recognise that no filter can guarantee to be 100% effective, however Surrey Teaching Centre are satisfied that our filtering system manages the following content and web searches:

Discrimination – Promotes the unjust or prejudicial treatment of people with protected characteristics of the Equality Act 2010

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

*This list is not exhaustive.

Surrey Teaching Centre recognise that filtering systems are only ever a tool in helping to safeguard children when online and we have an obligation to cover these areas within our curriculum where appropriate to the child/YP's current needs and abilities. These areas are outlined in our Personal Pathways curriculum and are recorded under this tab in the Evidence for learning platform. Curriculum content is supported by ProjectEVOLVE content.

How have Surrey Teaching Centre checked filtering to ensure it is robust and balanced?

- We have run a report on http://testfiltering.com/ as suggested by the UK safer Internet Centre to check our level of filtering.
- UK Safer Internet Centre recommends that schools undertake (and document) an annual online safety risk assessment, assessing their online safety provision that would include filtering (and monitoring) provision. The risk assessment should consider the risks that both children and staff may encounter online.
- A risk assessment module has been integrated in 360 degree safe. Surrey Teaching Centre have completed this auditing tool and have identified and recorded the risks posed by technology and the internet to their school, children, staff and parents.
- Eduthing have confirmed that Surrey Teaching Centre have:
- Offline backups of all critical information and systems, which are updated daily and stored securely off-site, this is using a backup solution called Redstor.
- A plan in place to handle any potential cybersecurity incidents. We take this seriously and want to make sure we're prepared for anything that might come our way.