ESafety Summary – KCSIE 2023 changes

(intended audience - Website)

Updated November 2023 by IT Manager

In KCSIE, there has understandably always been a heavy emphasis on eSafety, however in KCSIE 2023 there are some specific changes with regards to use and understanding of online filtering and monitoring tools. These systems are nothing new to us at Emmer Green, but invisible to most staff. The changes to KCSIE do emphasise the needs for the Designated Safeguarding Leads to be more aware of how this is all implemented. Here is a summary of some of the main points where this is addressed in KCSIE 2023;

1. The DSL has responsibility for "understanding the filtering and monitoring systems and processes in place" so this document will help to cover that requirement, explaining how these operate within the school, and the standards and processes we follow to keep things safe. Most of the content in this document aims to cover this requirement, hopefully in English!

2. Staff need to be given "an understanding of the expectations, applicable roles and responsibilities in relation to filtering and monitoring" in safeguarding and child protection training at induction. Staff have been recently given summary information on this subject, and ongoing updates should be given in upcoming staff/TA meetings to continue to cover and address this requirement.
3. It is stipulated that our child protection policy (Safeguarding Policy) should include details of how filtering and monitoring is part of our standard operating procedures to keep children safe when using technology within the school. These changes have already been made in the latest revision of our Safeguarding policy.

There are also some 'cyber security standards' that the school should work to meet. The detail in these is complex (and directed at internal IT teams and IT support provider types), but much of this is already covered in our IT policies, day-to-day practices used within the school, and in standards adhered to by the service providers we use for our internet access and filtering/firewall solutions. The appendix at the end of this document gives a one-line summary of each segment of those standards, though more detail is available in our internal policies and documentation!

Filtering and monitoring: How we do this at Emmer Green

We buy our internet connectivity from an Internet Service provider, just as you do at home. However, our provider specialises in schools' connectivity and the package we buy also includes comprehensive firewall and filtering systems, explained below;

1. Firewall – A network security device that monitors incoming and outgoing traffic and allows certain types of data in and out based on rules. It provides protection from cyber-attacks by shielding the school network from malicious or unnecessary network traffic. Think of it primarily as a line of defence from the outside, not to be confused with filtering.

2. Filtering – A solution that allows/blocks web browsing of certain websites based on page content, category, user, device, etc. It sits between your laptop and the internet, and stops users accessing certain URLs or websites by preventing pages from loading.

Firewall at EG

This is hosted and managed in our Internet Provider's data centres ('Schools Broadband' which is part of Talk-Straight). The firewall is set up according to industry best practice and school's standard requirements (which are very strict!). Changes can be requested by school if for example a new application or system we buy needs to communicate externally with the wider world (e.g. we may have to request opening 'ports' for a new phone system or external service provider that we exchange information with or through).

Filtering at EG

This is also hosted by Schools Broadband, and set up with a default and heavily restricted standard set of filters that all networked devices must adhere to. Web pages are classified by the system, with certain categories blocked by default (such as weapons, porn, hate speech, etc, etc). Page content and links are constantly monitored and updated by the system, making most safe browsing an uninterrupted experience for users.

Devices in school have software installed that allows the filter to determine whether the user is staff or pupil, with even heavier restrictions on the latter. If the software fails or a device does not have the software installed (for example a brand new device just being added to the network and yet to receive the installation) then access always defaults to the lowest possible access (which is pupil-level).

There are hundreds of generic categories included in our block/allow rules and the main ones customised for the school by internal IT are Pupil whitelist, Pupil blacklist, Staff whitelist and Staff blacklist. Staff can request that a site be added or denied to staff and/or pupils as appropriate, and after careful review it is added to the relevant list with information on why and when this is occuring.

Every web page visited by every device/user is logged on the system. Any attempts to visit blocked sites (user, machine , sites attempted, reason for block, date/time, etc) are included in access reports viewed daily by DSL and IT. Any attempts to visit blocked sites are investigated by IT and reported with conclusions back to DSL with explanation or follow-up tasks. For example a pupil may stumble across a 'Weapons' page (which would be blocked by the system and a report created), but if the teacher explains to IT when they report it that the pupil was writing a topic piece on medieval battles, then it is unsurprising that certain sites containing weapons (swords, shields, etc) may have be blocked by the filter.

Additional systems implemented through our internet provider give us a more immediate notification in more alarming cases, for example where a pupil has triggered the system with certain search keywords. In these situations, the system generates an instant 'Critical notification email' to DSL and IT allowing urgent action to be taken as appropriate.

Appendix 1: Filtering and monitoring standards for schools and colleges

Find out what standards your school or college should meet on filtering and monitoring.

From DfE 29-Mar-2023

Full text linked here: https://www.gov.uk/guidance/meeting-digital-and-technology-standards-in-schools-and-colleges/filtering-and-monitoring-standards-for-schools-and-colleges

EG summary answers below.

Task	Responsible
You should identify and assign roles and responsibilities to manage your filtering and monitoring systems	**SLT + Governor:** Responsible for ensuring standards are met. **IT Mgr:** Maintaining, reporting and actions relating to concerns and checks. Liaison with external service providers.
You should review your filtering and monitoring provision at least annually	**SLT + DSL + Governor + IT Mgr:** Perform and log annual safety review, creating actions as necessary.
Your filtering system should block harmful and inappropriate content, without unreasonably impacting teaching and learning	Using approved (Internet Watch Foundation) filtering provider, and devices/users set up according to best practice and vendor recommendations. All traffic logged and staff aware of process regarding safeguarding, technical concerns or requesting changes to allowed sites.
You should have effective monitoring strategies that meet the safeguarding needs of your school or college	Pupils not given unsupervised laptop access – staff supervision required. Filtering log reports reviewed and analysed daily. Critical safeguarding actions trigger instant email response to DSL and IT allowing immediate action. Site blacklists being constantly updated as necessary on top of sector-focused filtering solution. Monitoring system being implemented allowing screen viewing of all laptops in class by the teacher from front of class, with additional teaching features such as 'presenting' or showcasing a pupil's work on a laptop to the main class screen to the rest of the class.

Appendix 2: Cyber security standards for schools and colleges

Find out what standards your school or college should meet on cyber security, user accounts and data protection.

From DfE 29-Mar-023

Full text linked here: https://www.gov.uk/guidance/meeting-digital-and-technology-standards-in-schools-and-colleges/cyber-security-standards-for-schools-and-colleges

EG summary answers below. *(Much of this is covered in our annual Judicium Data Protection reviews)*

Task	Responsible
Protect all devices on every network with a properly configured boundary or software firewall	Industry leading firewall and filtering solutions installed as part of school internet connectivity package.
Network devices should be known and recorded with their security features enabled, correctly configured and kept up-to-date	Network PCs and servers patched and up to date. Monitoring systems identify machines accessing network and not 'patching' - IT action taken to remediate, rebuild, remove devices as appropriate. Printers, network switches, etc, all regularly updated with latest available firmware.
Accounts should only have the access they require to perform their role and should be authenticated to access data and services	All access determined by user role, with specific groups for pupils, staff, admin team, inclusion, SLT, HR, IT, etc.
You should protect accounts with access to personal or sensitive operational data and functions by multi-factor authentication	All staff accounts and email protected by MFA.
You should use anti-malware software to protect all devices in the network, including cloud-based networks	Industry leading cybersecurity software installed and actively monitored on all PCs and servers protecting against viruses, malware, ransomware, etc.
An administrator should check the security of all applications downloaded onto a network	Done. All users have non-administrative access to devices and are not allowed/able to install software on own devices without IT intervention.
All online devices and software must be licensed for use and should be patched with the latest security updates	All software patched and updated regularly.
You should have at least 3 backup copies of important data, on at least 2 separate devices, at least 1 must be off-site	3-2-1 backup policy in place for files, systems and servers.
Your business continuity and disaster recovery plan should include a regularly tested contingency plan in response to a cyber attack	Local and remote backups tested on regular basis for successful data restores.
Serious cyber attacks should be reported	Already part of our internal breach reporting process.
You must conduct a Data Protection Impact Assessment by statute for personal data you hold as required by General Data Protection Regulation	DPIAs are created and put in place for all new systems containing personal data.
Train all staff with access to school IT networks in the basics of cyber security	Part of staff induction, and regular updates in staff meetings, email circulars, etc.