Filtering, monitoring and cybersecurity at NKS

This document shows what is in place to meet the government requirements and associated statements from Keeping Children Safe in Education.
All staff and governors are updated on changed annually in the autumn term by either Lynsey Jones (DPO/DDSL) or Sarah Muldur (DSL/SENCO).

Government Standards	At NKS
Filtering and Monitoring	
Protect all devices on every network with a properly configured boundary or software firewall ***Checked and standard met***	Our firewall is provided by EXA and is specifically for schools. They control the rules and we do not have access. It can only be changed by 123ICT in consultation with EXA and by EXA when there is no option e.g. to allow a specific IP address through. The default password has been changed and is controlled by EXA. The firewall is restricted by EXA. As we (and 123ICT) have no access it does not require multi-factor authentication. Firmware is up-to-date and security support is current. Again, this is all provided by EXA. EXA constantly checks and monitors and makes changes when needed. It blocks all unauthenticated connections by default. It has been set up so we only receive the inbound traffic we need. It is regularly reviewed by EXA. As all networked devices access via EXA the firewall protects all devices. We are currently in the process of replacing all our managed switches and upgrading our internet.
Network devices should be known and recorded with their security features enabled, correctly configured and kept up-to-date ***Checked and standard met***	A list of all network devices is updated annually. This list includes make, model and security expiry date. It is compiled by our 123ICT Service Provider and through our Google for Education portal. All firmware is up-to-date mitigating against any high or critical vulnerabilities. Our router is provided by EXA, is up-to-date and kept up-to-date by them. Any internal switches and fibre have been checked and are up-to-date. Our wireless access points are updated termly or when critical by 123ICT. EXA provides protection to network devices to avoid a brute-force attack. We have a network diagram. One copy is kept by our 123ICT technician and the other by our school IT lead. We regularly remove or disable unused software and user accounts when staff and pupils leave. All devices are password protected and are using a password that is not the default one, this includes our CCTV. EXA and 123ICT have their own password policies for a network devices they support. Where an account has been compromised, we immediately block the account and then we work with 123ICT to support the account holder with recovery where possible, clean up and creating new security levels.
Accounts should only have the access they require to perform their role and should be authenticated to access data and services ***Checked and standard met***	All accounts have the access they require via our Google Management system. There is no network separation as we have no separate VLAN and instead allow individual users access to what they need via our separate Google Drive folders. Multi-factor authentication is in place for all staff users accessing GDPR regulated data.

You should protect accounts with access to personal or sensitive operational data and functions by multi-factor authentication (MFA) ***Checked and standard met***	All networked devices are password protected as are all accounts with access to our school Google Drive. We have multi-factor authentication for CPOMs, Arbor and Outlook/Office 365. Staff save all school related work to their secure Google Drive. IT lead and several other members of staff have multi-factor authentication on their additional accounts. All laptops are set up with a Teacher and Admin account. The laptops are not individually recognisable and therefore this provides an extra deterrent when trying to force access.
You should use anti-malware software to protect all devices in the network, including cloud-based networks ***Checked and standard met***	Anti-malware is provided by EXA and 123ICT install it in addition onto any networked devices as needed. Our antivirus is provided by Microsoft. This is regularly checked by out 123ICT technician.
An administrator should check the security of all application downloaded onto a network ***Checked and standard met***	No user is allowed to download anything to their staff laptop without consultation with school IT lead or 123ICT. When they are downloading, staff have been made aware of checking for hidden installs. If this is proven to be ineffective, we will insist that only 123ICT can download on staff devices. This would be a last resort as doing this would have an impact on teaching and learning.
All online devices and software must be licensed for use and should be patched with the latest security updates ***Checked and standard met***	All Chromebooks are monitored through our Google for Education Management Portal. They are all licenced for use and up-to-date with security patches. All other networked devices are licenced and up-to-date with security patches. They are checked annually when our asset register is checked. Our iPads are all monitored by 123ICT using Mosyle which allows us to see when they are out of support/security updates. We have a rolling program in place to replace Chromebooks and iPads. 2 chromebooks out of support – These has been given to members of staff to only use for accessing Twinkl and White Rose only but are on order to be replaced . 123ICT ensures all firmware is up-to-date mitigating against any high or critical vulnerabilities and this update happens regularly throughout the year. Where necessary 123ICT support us with ensuring all installed software is up-to-date. The teaching and learning software we use is all cloud based and therefore up-to-date with security settings and patches.
You should have at least 3 backup copies of important data, on at least 2 separate devices, at least 1 must be off site ***Checked and standard met***	We have multiple backup copies as required. Our data is stored in Integris and within our Google Cloud.

Your business continuity and disaster recovery plan should include a regularly tested contingency plan in response to a cyber attack ***Checked and standard met***	Our school plan includes how we react to a cyberattack. If the compromise is to a single networked device, it will be removed from the Wi-Fi, isolated and 123ICT will be contacted. If the compromise is on a wider scale 123ICT will be contacted who will support the school with next steps. Our main data is in the Google Cloud, within the RM Integris system or via online providers who and they have Cyber security information on their website. An annual test will take place each December.
Serious cyber-attacks should be reported ***Checked and standard met***	We would report this and 123ICT would help assist recovery.
You must conduct a Data Protection Impact Assessment by statute for personal data you hold as required by GDPR ***Checked and standard met***	A Data Protection Impact Assessment would be carried out as required when we are undertaking a large project. The information about Data Protection can be found on our GDPR audit which is updated annually and added to when needed.

Cybersecurity

You should identify and assign roles and responsibilities to manage your filtering and monitoring ***Checked and standard met***	Lynsey Jones - DDSL, DPO, GE Level 1 and IT lead Nick Speller - 123ICT (external service provider), CEOP Ambassador and 360 Safe Assessor, GE Level 1 and 2 and certified Trainer Dr Reip – Governor Sarah Muldur – DSL and SENCO
You should review your filtering and monitoring at least annually ***Checked and standard met***	Occurs annually in the autumn term. Monitoring and adjustments to filtering happens ongoing throughout the year.
Your filtering system should block harmful and inappropriate content, without reasonably impacting teaching and learning ***Checked and standard met***	EXA provides our filtering (Quantum). They fulfil the following criteria: • Are a member of Internet Watch Foundation (IWF) • Are signed up to Counter-Terrorism Internet Referral Unit list (CTIRU) • Are blocking access to illegal content including child sexual abuse material (CSAM) The decisions about filtering are put in place by them adhering to all government requirements. If we come across something we believe is inappropriate, we send the url/information to 123ICT who will contact EXA to have it filtered out. The same applies if we have a query or need to make an amendment.

You should have effective monitoring strategies that meet the safeguarding needs of your school or college ***Checked and standard met***	Our school uses physical monitoring to ensure we keep children safe online. No child is left unattended when online. ESafety is taught discretely and embedded into our curriculum and is not solely addressed in computing sessions. Our IT Lead and 123ICT Service Provider work together annually to lock down children's Google accounts to minimise what children can do when on a networked device. Children's accounts open straight onto our school hub which points children in the direction of sites that are safe and for their use. Sanctions are in place for children found abusing their ability to work online.