Smoothwall Implementation
Update Document 16 October 2023

1.	**What is Smoothwall Monitor?**
	Smoothwall is a monitoring software that has the capability to capture words of concern typed into internet browsers. Smoothwall **does not** monitor apps.
2.	**What is the reason for implementing Smoothwall Monitoring?**
	Inline with Keeping Children Safe in Education 2022 schools must have an appropriate monitoring system in place. The monitoring is to protect against the exposure to illegal, inappropriate, or harmful content, for example; pornography, fake news, racism, misogyny, self-harm, suicide, anti-Semitism, radicalisation, and extremism. With the online world developing at such a rapid pace, especially since the start of the pandemic, schools across the country are seeing an increase in issues arising from online risks. In response to this, the academy will be implementing '**Smoothwall Monitor**' which is a leading software to highlight to school leaders any safeguarding concerns. Concerns will be identified through '*keystroke monitoring*' and '*screen capture*'. In simple terms, this means that if someone accessing our IT network types in certain words, a report will be sent to the school leader flagging that the user may be in need of support. The intention is to ensure that we are doing everything we can to protect our school communities from online risk and ensure that anyone in need of mental health or emotional support is identified as quickly as possible. *The purchase of this software has been undertaken with the inclusion of IT specialists. We feel that this is the best option for our Trust.*
3.	**What will Smoothwall 'monitor'?**
	Smoothwall will monitor any work/school or approved device accessing the internet whether they are used at school or home. We will operate this software in line with our Data Protection (UK GDPR) Policy and our Privacy Notices, and any concerns that are flagged will be dealt with under strict confidentiality.
4.	**What is the legal basis for this software?**
	Public task. In accordance with *Keeping Children Safe in Education 2022 points 141 and 142, and the Safer Internet Centre's guidance at* https://saferinternet.org.uk/guide-and-resource/teachers-and-school-staff/appropriate-filtering-and-monitoring/appropriate-monitoring
5.	**Is the implementation just at Manor CE Academy or Trust wide?**

	As stated above, the implementation is inline with Keeping Children Safe in Education 2022. As this relates to all educational establishments, this is Trust wide.
6.	**Who is reviewing the data Smoothwall captures and what can they see?**
	There is no automated decision making as all results pass through human moderation in 2 stages. **Employees for Smoothwall** UK, DBS checked with senior staff vetted to NPPv3. Fully employed by Smoothwall Initial period of training to familiarise with systems and processes, followed by a longer period of training with sample data sets. Continuous professional development to ensure quality and that their knowledge of emerging risks and threats is current. *The full training policy is commercially sensitive.* Moderators see the captured text, screenshot, username and school DSL contact details. They can also review the previous 24 hours captured text from that user, but not the screenshots. All colleagues are given an initial period of training to familiarise with systems and processes, followed by a longer period of training with sample data sets. Continuous professional development to ensure quality and that their knowledge of emerging risks and threats is current. Moderators see the captured text, screenshot, username and school DSL contact details. They can also review the previous 24 hours captured text from that user, but not the screenshots. **Trust Employees** The Smoothwall monitoring system will only be accessed by key members of staff i.e. Principal, Designated Safeguarding Lead and/or appropriate staff with safeguarding responsibilities. This limits the access to such information.
7.	**Devices are not owned by the school. They are either 1) part of a lease agreement, where the school is not the lessor, or 2) are purchased and owned privately by families. How do you handle deployment of Smoothwall Monitor with this level of BYOD with other customers?**
	It has been agreed, based on the installation of the mobile device management software and Smoothwall monitoring, personally owned Ipads will be permitted on the system. This decision has been made due to parental feedback that Ipads may have now been fully purchased and used by their children or passed down to a sibling. As the mobile device management software will be in place, we will not require a 'Bring Your Own Device Agreement' For those who refuse to permit the mobile device management software and smoothwall to be installed on their devices, will not be permitted within school.
8.	**Does the software 'profile' users?**
	It does **not** create a profile of the individual. It creates a profile of the captures which enables the software, if applicable, to establish the potential risk.

9.	**What software is installed on each iPad, and what does each component do?**
	The software is a browser-replacement on iPad, where the keystroke input in the browser is assessed via a cloud-based system for potential safeguarding risks. If the cloud-system determines based on textual rules that the content is of concern, a screenshot is captured and is placed in a queue for human moderation. Depending on the human moderation result, the content may be placed in the School's portal for review, or escalated to a DSL by email/phone if it is of high risk or there is an imminent threat to life.
	Depending on the configuration and licensing of the organisation, the browser may also perform web filtering using the Smoothwall Filter product, where each web page accessed is analysed locally on the device for content which is in breach of the defined policy. If in breach, the page will be blocked with an appropriate message displayed. Activity logs of browsing will be available for the school.
	Operation of Monitor and Filter differs on Windows, Mac and ChromeOS*
	It is assumed that these questions only relate to iOS.
10.	**If you are installing, for example, an alternative browser, will Safari/other browsers be disabled?**
	Smoothwall Monitor does not itself disable other browsers, this would be a function of Mobile Device Management (MDM), proposed solution being JAMF, and controlled by the device administrator.
	During the school linked times, other browsers will be disabled. These will become available once the time period for school based activities has ended.
11.	**What monitoring is done on other applications installed on the device?**
	None.
12.	**Explain specifically what 'keystroke monitoring is'? Are all keystrokes recorded, or just some apps? How do you prevent collection of private data (e.g. personal data (not related to school), passwords).**
	On iPad this relates to any interaction between the keyboard and a web page in the replacement browser application. Only keystrokes within the replacement browser are captured. Various rules exist to detect data such as credit card numbers, passwords and so on based on the format of the capture and where it is entered (for example into a "password" input form on a website, or if the website page is titled 'Login'). Lists of sites where data is never to be captured from are also maintained.
13.	**Explain specifically how the 'take a screenshot' works? What triggers this? How do you ensure you are not taking screenshots of private data, e.g. (non-school related email, web browser, banking information, health information, shopping (specifically around PCI compliance). As you are only the**

	data processor, are the Academy Trust aware they could be liable for being the Data Controller for this type of data?
	When the keystrokes are captured, a capture of the entire browser tab contents is stored. If the cloud system determines that the capture is of interest, then the screenshot is transferred – otherwise it is destroyed. The rules mentioned in the previous point can help avoid capturing sensitive data, however inevitably data of this nature may be captured, particularly with the purpose of the system being to help identify safeguarding risks associated with the students' wellbeing.
14.	**The solution uses 'AI' Explain more about this? Does this run on the device?**
	It is a sophisticated collection of text-based rules that run in the cloud, supplemented by a smaller set of redaction rules that run locally on the device.
15.	**Does Smoothwall support disabling the 'AI', as GDPR allows the right to withdraw consent for automated processing and decision making?**
	There is no automated decision making as all results pass through human moderation, both our own and the determination of risk that the school DSL makes upon receiving any alerts. As this implementation is based on '**Public task**' there is **no** requirement for consent.
16.	**Is the Data encrypted?**
	Yes, both in transit and at rest.
17.	**Who holds the encryption keys**
	Smoothwall and Microsoft
18.	**When was the last Security Audit and Pentest of the software platform carried out? Have all findings of that been implemented/mitigated?**
	Security Auditing and Penetration Testing are implemented as automated continuous processes. All historic findings have been resolved. We have investigated a concern raised by a parent/carer and have provided the outcome with Q20.
19.	**Parents/Carers raising what they consider to be security issues on the Smoothwall website and Smoothwall Express Product**
	The Smoothwall website, along with other websites in their global organisation, undergo regular checks by the global security team to ensure they remain robust and compliant with the latest standards. In the case of the UK Smoothwall website, the issues were caused by their third party hosting provider who had regressed some changes. A subsequent scheduled scan would have picked this up but we thank those parents/carers for bringing this to our attention. This has now been resolved.

	Smoothwall Express is not related to Smoothwall, even though they use the same name. The background is explained, by Smoothwall, below so parents/carers are aware:-
	"Our company Smoothwall started life as an engineer-led open source, firewall project back in 2000. In 2001 Smoothwall Ltd was formed to offer a proprietary commercial version of the open source product, led by the same engineering founders. The open source project at that point became known as Smoothwall Express. The founders worked on both the open source and commercial products together until 2014 when the two entities separated. *Since then, Smoothwall Ltd has had no involvement in the open source project, and has developed many, entirely unrelated products (Smoothwall Monitor being one). Any vulnerabilities that may have existed in Smoothwall Express have long been resolved in our commercial products"*
20.	**What software is installed on each iPad, and what does each component do?**
	Mobile Device Management Software - Proposed JAMF instead of LIGHTSPEED This enables 'policies' to be added to the device i.e. only use Smoothwall Monitor on school days and during specified hours. The policies will be defined by the Trust to ensure that we comply with Keeping Children Safe in Education 2022. This is a safeguarding tool therefore will only be focused on the activity within the school day. **Smoothwall Monitoring** Detailed above.
21.	**Why do we need to backup and wipe the iPad before the installation of Smoothwall ?**
	The way management profiles are applied to iPads, as required by Apple©, is that they are applied during the initial setup of the device. As such, the devices need to be wiped. Once in the setup, they connect to the internet for the first time and check in with Apple to see if there is a profile applied to the device; if so, it will configure the device in that manner. A backup will be taken before the wipe so once they have gone through the setup process, all the data can be re-downloaded from iCloud or the Google drive, depending on how the backup was taken.
22.	**If you are installing, for example, an alternative browser, will Safari/other browsers be disabled?**
	Utilising effective Trust policies, we will be able to permit alternative browsers outside the monitoring hours.
23.	**What monitoring is done on other applications installed on the device?**
	None.
24.	**If the IPad our children are using is supplied by us and we don't want the Smoothwall software adding due to the restrictions which will be enforced, how will they continue their education within the school and future revision/homework/projects**

	The Ipad scheme is operated by the school to support the educational experience of your children. This is therefore a linked scheme and MDM software is stated within the correspondence to parents/carers prior to signing up for the scheme.

If parents/carers do not want their Ipads included within this software implementation then new scheme devices will not be permitted and existing scheme devices will unfortunately not be able to be used within the school.

We regret that this is the case, but as the monitoring of our internal IT systems is required, we have no alternative but to ensure compliance for the safety of our students. |
25.	**How long is the data kept for?**
	Unless the capture relates to a specific safeguarding situation relating to the student which is required to be retained by law, captures will be deleted after 12 months
26.	● **How and where information will be stored, access to this and safeguards to protect this information from misuse.** ● **Can you advise how you will protect our children from 'teachers room gossip' spreading to the classroom and beyond?** ● **Who and what role(s) within Manor Academy will have access to the proposed data captures?** ● **How is a young person's right to privacy and confidentiality to be protected say for example when searching for information on gender identity or sexual orientation. Protection against the risk of being 'outed' is essential. What sort of information is to be inferred?**
	The Smoothwall monitoring system will only be accessed by key members of staff i.e. Principal, Designated Safeguarding Lead and/or appropriate staff with safeguarding responsibilities. This limits the access to such information.

Should a student be searching for such information relating to gender identity or sexual orientation, there may be a need for support and assistance to be provided. |
27.	**The Information Commissioner's Office advises that under their right to be informed you must provide children with the same information about what you will do with their personal data as you give to adults. When will the children be consulted? Will this consultation be given under correct requirements in a way they can fully understand.**
	As a **public task**, we have a responsibility to protect our students. Consultation is not required under this legal basis. However, we will be requesting that schools provide delivery of either an assembly or a lesson relating to PHSE to ensure that they are informed.
28.	● **What happens to data captured when a child leaves Manor Academy / the Trust?** ● **What is the need/justification for storing data for 12 months after leaving school - is this legitimate and compliant with GDPR.**

	Unless the capture relates to a specific safeguarding situation relating to the student which is required to be retained by law, captures will be deleted after 12 months.
	There may be a situation that requires a review of the captures due to a known or unknown safeguarding concern. Under GDPR, we only retain information for a limited period to ensure that this can be accessed if requested by the Police or other official agencies.
29.	**How will positive results be handled?**
	These will be handled by a nominated member of staff i.e. Designated Safeguarding Lead, Head of Year; someone with designated safeguarding responsibilities for your child. The action will be appropriate to the capture which may include an initial discussion to establish further information.
30.	**How will students be identified on the date capture?**
	This will be via their school username which, in *confirmed* solution, will be linked to their AppleID.
31.	**Will any previously bought / downloaded plugins still work with the new browser? Eg for SEN support etc**
	Yes. We are developing the procedures to ensure that all apps relating to the Apple Personal ID are retained.
	We would request that parents/carers if a specific app has been purchased for the educational support for their child, we would request that you email **dpo@hslt.academy** subject titled 'Specialist App' and provide the full details; we will respond on an individual basis.
32.	**This would mean my daughter losing work she has already completed for GCSES which is unacceptable.**
	This should not be the case. Details of software applications/apps being used to be provided.
	We would request that you email **dpo@hslt.academy** subject titled 'Software/Apps Notification' and provide the full details; we will respond on an individual basis.
33.	**What process(es) do you have in place (for those roles) for handling the subject access requests from the solution; and the size of data captures?**
	This will be inline with the Trust policy. In circumstances where checks need to be made on specific 'subjects' the DPO will work with the IT specialist to gain the information.
34.	**The DPIA talks of levels of captures, 1-5 ,what are examples of these levels and what is the typical scenario as to how the concerns they might raise be addressed.**

	There is no typical scenario. However, in the first instance and in a 'general' issue being raised. An appropriate member of staff will discuss the findings with the student. If it is deemed necessary/appropriate, the parents/carers will be informed.
35.	**Can my child use their Ipad under the 'Bring Your Own Device' policy without the monitoring.**
	Unfortunately not.
36.	**What happens if all parents/carers with existing Ipads on the scheme do not permit the implementation of the MDM and Smoothwall Monitoring?**
	The Ipads will not be permitted to be used within the school environment. The school has a 'pool' of Ipads that can be used but this is limited in number. If the numbers are significant a formal review of the Ipad scheme will be undertaken.
37.	**Will the Trust commit to a 1 to 1 Ipad device for students if parents/carers refuse to support the implementation of Smoothwall.**
	The Ipad scheme was historically established as an enhancement to the students educational experience. The funding of educational establishments is based on curriculum delivery and does not include the ability to provide an Ipad for every student. The Trust has moved to Google for mainstream devices which would result in Manor having to change significantly in the way they teach and learn. Some existing programmes do not operate on chromebooks. We are therefore implementing a Trust initiative to enable access to devices for all students, but this will be a phased approach over the next 3 to 5 years. If we need to review the IPad scheme at Manor, this will take a considerable amount of time. In this instance we will engage with parents/carers to establish a working group.
38.	● **Changing the contract so far through is also unacceptable. If you feel the need to change, start with year 7.** ● **I still strongly disagree with the installation of the new software, so many apps the children use regularly in and out of school will not be available.**
	Schools must implement an effective monitoring provision inline with Keeping Children Safe in Education. We need this to be school wide. As a legislative requirement, this is under a public task.
39.	**Also had this been used during lockdown the children would not have been able to communicate with each other so well which was vital under such circumstances.**
	This will not prevent communication between individuals.
40.	**What about trust which is one of the core values of the school.**

	This is a required safeguarding measure inline with Keeping Children Safe in Education. Safeguarding is a known concern within educational establishments nationally and therefore taking steps to ensure the safety of students within our care is core to our values.
41.	**Is the data processed on the device, or the cloud?'**
	The cloud.
42.	**You state 'Smoothwall Monitoring has been established as a proportionate measures that enabled time critical evidence in the mitigation of and/or reduction of safeguarding risks'** **Please provide evidence to your statement that the proposed solution 'has been established as a proportionate measure[s]'**
	Please refer to:- **https://saferinternet.org.uk/guide-and-resource/teachers-and-school-staff/appropriate-filtering-and-monitoring/monitoring-providers-responses**. In addition, during an Ofsted inspection, schools may be required to demonstrate effective monitoring of students' use of IT for reasons relating to safeguarding.
43.	**There have been a lot of rumours floating around about what children will and won't be able to do on their ipads once smoothwall is installed. The latest email says that the software will only be active during school hours, during the school term. Just to clarify, does that mean that all apps including those such as BBC iplayer, Netflix, Youtube and the odd game will still be able to be installed on the ipads and usable outside school hours, just disabled within school?**
	Just disabled during the school timings set by policy (*confirmed 0800-1630*). The school term dates will be logged into the system. The only exception that may involve the monitoring while at home is during absence from school; unfortunately, this cannot be individualised.