

Monitoring System Review

Details

Monitoring Provider:

.....

System Name:

.....

Date Procured:

.....

Date of Last Review:

.....

Previous Review:

Date:

Review Conducted By:

Include names of the senior leadership team (SLT) member responsible for filtering and monitoring, the designated safeguarding lead (DSL), IT support, and the responsible governor.

The review should be informed by:

- Student risk profiles: number and age range of your students, device access and frequency, SEND, EAL, digital resilience..etc.
- Your local safeguarding context, such as county lines
- Relevant safeguarding reports or serious incidents
- Teaching requirements, such as RHSE or PSHE
- How your setting uses technology, e.g. BYOD or generative AI tools
- Related safeguarding or technology policies
- Checks currently taking place and how resulting actions are handled
- Technical set-up recommendations to make sure the system works effectively
- The structure of your organisation and safeguarding team

Monitoring checklist:

Tick each statement that reflects your current monitoring provision.

- ☐ Our monitoring system picks up incidents of concern urgently, allowing us to take prompt action and record the outcome
- ☐ Our monitoring provision identifies and alerts us to behaviours associated with the 4 areas of risk outlined by [KCSIE](#): content, contact, conduct and commerce
- ☐ We have assessed whether our monitoring system can handle real-time, dynamic, personalised and AI-generated content, and identified any technical limitations
- ☐ We have assessed the risks of any generative AI tools used in our setting, referring to the DfE's [Generative AI: product safety standards](#)
- ☐ We have a clear monitoring plan that details how students (and staff, if applicable) are monitored when using school/college-managed devices
- ☐ Monitoring systems are confirmed to work on new devices and services before they are released to staff and students
- ☐ Users must authenticate on managed devices, so concerns can be traced back to an individual, including guest accounts
- ☐ Monitoring data is received in a format that our staff can understand
- ☐ Our DSL(s) and IT support receive training on the management of technical monitoring systems to ensure their knowledge is current
- ☐ We have a documented process for recording incidents that includes actions taken and the outcomes
- ☐ Our monitoring procedures and systems are reflected in our acceptable use policy (AUP)
- ☐ Staff conduct a level of in-person monitoring if they are in a room with students on devices
- ☐ All staff know how to report and record monitoring-related concerns, and understand when incidents should be acted on, in line with our school/college's policy
- ☐ Our monitoring strategy includes (at least) weekly monitoring reports highlighting incidents
- ☐ Incidents classed as high-risk produce immediate reports
- ☐ We have conducted a [data protection impact assessment \(DPIA\)](#) and review the privacy notices of third-party providers

Reflective questions

Question	Answer
Do you have “effective monitoring strategies that meet the needs of your school or college”?	
Which monitoring strategy do you use and why?	
Do safeguarding and technical teams work together to deliver effective monitoring?	
Are senior leaders, governors, school staff, students and parents/carers aware of the monitoring strategy in place and the rationale behind it?	
How are monitoring incidents, responses and results recorded in existing reporting systems?	
Who deals with monitoring alerts? Do they also use monitoring data to identify concerning trends or to inform school/college curriculum?	
What are the technical limitations of your monitoring system, including with real-time, dynamic, personalised or AI-generated content?	
How do you keep false positives on your monitoring system to a minimum?	

Monitoring System Checks

Record every check carried out across the year (not just at review time) so this log can be shown to anyone entitled to inspect it.

Date checked:

Conducted By:

[illegible]

Monitoring System Review Outcomes

Reflections on results/outcomes/planned improvements

Date of next review:

Note: This template is a general guide and may not cover every step your monitoring review should include. What's required will depend on your setting's specific configuration, needs and risk profile, so it should be adapted and used alongside your own judgement, that of your DSL, IT support and governing body, and the full [KCSIE 2026 guidance](#) and [filtering and monitoring standards](#). It is not a guarantee of compliance.

Smoothwall Monitor can help you firmly establish an effective digital monitoring strategy in your school, college or MAT.

To learn more or book a demo, contact enquiries@smoothwall.com.

We're ready to help.