

# School Governors Digital Monitoring Checklist



Having the right monitoring tools in place to fulfil duty of care is vital for schools and Multi Academy Trusts. Securus offers protection on ALL devices and applications, ensuring the welfare and well-being of pupils and safeguarding against concerns such as bullying, racism, sexual exploitation, radicalisation, hacking, mental health & well-being, hate speech, suicide and self harm, substance abuse and gang culture to name a few. This checklist has been produced to support Governors in their role of Digital monitoring & safeguarding!

## Roles of the School Governors

Governors have an understanding & knowledge of the monitoring provision in place

Governors are sent regular reports on safeguarding incidents, trends and alerts

Governors are involved in the review and approval of all child protection & safeguarding policies, providing support & input

All Governors assess and provide input on the effectiveness of the monitoring solution

Governors are involved in decisions regarding procurement and review of the monitoring provision

Governors understand the statutory requirements of Keeping Children Safe in Education guidance, the Prevent duty, Filtering and monitoring standards, working together to safeguard children and the Online Safety Act

Governors have the relevant safeguarding training with the latest legislative updates, trends & terminology to reflect policy and practice

The monitoring provision is compliant with the DfE's Keeping Children Safe in Education guidance/Prevent duty and current legislation

The Designated Safeguarding Lead has robust knowledge of, Online Safety and the role and responsibility held

The Designated Safeguarding Lead has received appropriate training in the last 12 months

Ensure the school has a clear, effective policy on mobile phone usage and that this policy is implemented regularly, understood and reviewed for student behaviour, safety, and wellbeing

Governors must understand & ensure AI is used safely, ethically, and strategically, focusing on policy implementation, data security, and compliance

Governors carry out an Academic Annual Review of effectiveness with a time frame given

## Review Process

The Online Safety Policy/Child Protection Policy is in place and has been reviewed and updated in the last 12 months

The Acceptable Use/Behaviour Policy is in place and has been reviewed to accommodate technology and online behaviour

All staff understand their responsibilities regarding Online Safety and have received Online Safety training

Robust reporting is in place for Online Safety concerns & incidents

All students understand their Online Safety Rights & Responsibilities and clearly understand how to appropriately report concerns

All staff (teaching and non-teaching), volunteers and supply staff clearly understand what to do if an incident occurs or is reported

Regular engagement takes place with parents/carers about Online Safety and they are aware of the School/College's Acceptable Use/Behaviour Policy and have received/returned the internet access permission form

ALL students are aware of and understand the use of the monitoring provision in place and the AUP

Students are educated about Online Safety as part of the curriculum

Provisions are in place for SEND students and those with sensory support and needs/vulnerabilities so they understand online safety and acceptable behaviours

Students/staff & parents are aware of policies in place for mobile phone use with clear guidance

Students are educated on the safe use of AI and understand school policies

A backup safeguarding lead is in place for absence and cover

