# Filtering and Monitoring

# Checklist Register

In line with the [DfE filtering and monitoring standards in schools and colleges](https://www.gov.uk/guidance/meeting-digital-and-technology-standards-in-schools-and-colleges/filtering-and-monitoring-standards-for-schools-and-colleges), this checklist template has been developed as a basis to support schools and colleges in meeting the required standards. Whilst not intended to be exhaustive, this resource can serve as a summary record of checks highlighted within the standards.

|  |  |  |
| --- | --- | --- |
| Last updated: | **Date:** | **Name/Position:** |

# Roles and Responsibilities

|  |  |  |
| --- | --- | --- |
| Role | Responsibility | Name / Position |
| Responsible Governor | Strategic responsibility for filtering and monitoring and need assurance that the standards are being met.   |  |
| Senior Leadership Team Member | Responsible for ensuring these standards are met and:* procuring filtering and monitoring systems
* documenting decisions on what is blocked or allowed and why
* reviewing the effectiveness of your provision
* overseeing reports

Ensure that all staff: * understand their role
* are appropriately trained
* follow policies, processes and procedures
* act on reports and concerns
 |  |
| Designated Safeguarding Lead | Lead responsibility for safeguarding and online safety, which could include overseeing and acting on:* filtering and monitoring reports
* safeguarding concerns
* checks to filtering and monitoring systems
 |  |
|  IT Service Provider | Technical responsibility for:* maintaining filtering and monitoring systems
* providing filtering and monitoring reports
* completing actions following concerns or checks to systems
 |  |

# Reviewing your filtering and monitoring provision

|  |  |
| --- | --- |
| Filtering System |  |
| Filtering Provider and System |  |
| Date Procured |  |
| Date last reviewed |  |

|  |  |
| --- | --- |
| Monitoring System |  |
| Monitoring Provider and System |  |
| Date Procured |  |
| Date last reviewed |  |

|  |  |
| --- | --- |
| Review Team[should be conducted by members of the senior leadership team, the Designated Safeguarding Lead (DSL), and the IT service provider and involve the responsible governor] |  |
| Review Date |  |
| Previous Review Date |  |
| Link to last review |  |
| Review Checklist |
| the risk profile of your pupils, including their age range, pupils with special educational needs and disability (SEND), pupils with English as an additional language (EAL)  |  |
| what your filtering system currently blocks or allows and why |  |
| any outside safeguarding influences, such as county lines |  |
| any relevant safeguarding reports |  |
| the digital resilience of your pupils |  |
| teaching requirements, for example, your RHSE and PSHE curriculum  |  |
| the specific use of your chosen technologies, including Bring Your Own Device (BYOD) |  |
| what related safeguarding or technology policies you have in place |  |
| what checks are currently taking place and how resulting actions are handled |  |

|  |  |
| --- | --- |
| all staff know how to report and record concerns  |  |
| filtering and monitoring systems work on new devices and services before release to staff / pupils  |  |
| blocklists are reviewed and they can be modified in line with changes to safeguarding risks |  |

|  |  |
| --- | --- |
| Recommendations / Mitigating Actions |  |
|  |

# Data Protection Impact Assessment

Schools and colleges that have a technical monitoring system will need to conduct their own Data Protection Impact Assessment (DPIA) and review the privacy notices of third party providers

|  |  |
| --- | --- |
| Link to DPIA |  |
| Conducted by |  |
| Date conducted |  |

# Regular Reports

|  |  |
| --- | --- |
| Type of Report | Filtering / Monitoring |
| Producer of report |  |
| Recipient of report |  |
| Frequency of report |  |

|  |  |
| --- | --- |
| Monitoring data is received in a format that your staff can understand  |  |
| Users are identifiable to the school / college, so concerns can be traced back to an individual, including guest accounts   |  |

# System Checks

|  |  |
| --- | --- |
| **Filtering System** |  |
| Date checked |  |
| Checks conducted by |  |
| Device | Location | Logged in as | Check Conducted | Result |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |

|  |  |
| --- | --- |
| Confirm your filtering provider is:  |  |
| * a member of Internet Watch Foundation (IWF)
 |  |
| * signed up to Counter Terrorism Internet Referral Unit list (CTIRU)
 |  |
| * blocking access to illegal content including Child Sexual Abuse Material (CSAM)
 |  |

|  |  |
| --- | --- |
| **Monitoring System** |  |
| Date checked |  |
| Checks conducted by |  |
| Device | Location | Logged in as | Check Conducted | Result |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |

SWGfL© 2023