OUR LADY IMMACULATE CATHOLIC ACADEMIES TRUST

ST JOHN RIGBY PRIMARY SCHOOL

God's will be done through work and play, as we follow Jesus day by day

SJR Filtering & Monitoring Statement

Filtering and Monitoring Information

The internet is used daily across our curriculum and is a key learning tool for pupils. At the same time, pupils may be exposed to potentially harmful material. To safeguard pupils and meet our statutory duties (including the Prevent duty and Keeping children safe in education 2025), the school operates comprehensive filtering and monitoring across all school-owned devices and the school network.

Content filtering works by applying specific parameters to content retrieved via the internet, restricting access to certain materials on websites, Apps, emails or other suspicious items. It can be a hardware or software solution and can often be part of a firewall setting.

Monitoring combined with content filtering alerts for any activities that need to be acted upon, but the information is also used to determine which sites and keywords need to be filtered out. For example, if a new craze appears, the monitoring and filtering system will help us know what associated terms the children are searching for, and what websites they are accessing.

To safeguard and promote the welfare of our children, we provide them with a safe environment in which they can learn and flourish, by ensuring that they are not exposed to any online risks associated with using the internet.

Technology in use
The school use Securly as our primary cloud-based web filtering and monitoring provider. Technical integration, device management and day-to-day configuration for Securly are delivered in partnership with OLICAT IT Services and the Trust's central IT provision to provide:

- cloud web filtering applied across the school network and to school-managed devices (on- and off-site where device management is applied);
- HTTPS inspection where required to check encrypted traffic while balancing privacy and safeguarding needs;
- AI-assisted categorisation and sentiment analysis to detect safeguarding risks in searches and online activity (for example self-harm, sexual content, radicalisation, bullying, hate speech);
- real-time alerts for high-risk activity and dashboards/automated reports for DSLs and senior leaders;
- reporting dashboards and automated reports to support DSLs and senior leaders in reviewing online-safety incidents and patterns.

To ensure all standards are met we will:

1. Assign roles and responsibilities to manage the filtering and monitoring systems

Strategic responsibility:
Our Trust Directors and Local Academy Committee have overall strategic responsibility for filtering and monitoring and need assurance that the standards are being met.

Operational Leads:
- Headteacher / DSL — Mrs M McGettigan: accountable for ensuring appropriate responses to alerts and safeguarding concerns identified via Securly.

- Safeguarding Governor — Mrs I Bond: responsible for receiving assurance about effectiveness and annual review outcomes.

- OLICAT IT Services (Trust IT): responsible for Securly configuration, secure logging, updates and technical resilience.

- All staff: responsible for following online-safety routines, using classroom-management tools appropriately and reporting concerns through school safeguarding procedures.

2. Consider filtering configuration and curriculum needs
Securly is configured to block access to clearly harmful and inappropriate content for our pupil age profile (including pornography, extremist material, illegal content and other categories identified in KCSIE 2025).

Filtering categories are set to balance safeguarding with legitimate curriculum use. Staff may request category changes or temporary curriculum whitelists through OLICAT IT Services. All such requests must be authorised by SLT and logged with reasons and duration.

Any permanent exceptions are recorded and reviewed at least termly.

3. Conduct monitoring, alerting and triage
Securly monitoring covers activity on school-managed devices and accounts. This includes web searches, visited URLs and, where enabled and appropriate, flagged content within cloud accounts associated with school-managed services.

High-risk alerts are sent to the DSL (or delegated safeguarding staff) for immediate triage and action. The DSL records actions and outcomes in the school's safeguarding system CPOMS.

Routine reports and dashboard views are reviewed by the DSL to identify trends, repeat concerns, or pupil-level escalation needs.

Where devices are school-managed, Securly protections apply off-site in line with the agreed device-management configuration.

4. Ensure data protection, privacy and proportionality
Monitoring is lawful, transparent and proportionate. We will ensure:

- access to Securly alerts and pupil-level data is restricted to authorised staff (DSL, deputies, headteacher and relevant SLT) and logged/audited;
- retention of logs and reports is limited to what is necessary for safeguarding or statutory reasons and handled in line with the school's retention schedule;

- classroom-monitoring tools are used to support teaching and safeguarding, not to undertake unnecessary intrusive surveillance of pupils or staff.

5. Integration with safeguarding procedures
Alerts and incidents identified by Securly are managed through the school's child-protection procedures. DSLs will:

- triage alerts, take immediate safeguarding action where needed and record outcomes;

- make referrals to external agencies (police, children's social care) without delay when appropriate;

- use Securly trend data to inform prevention work, pupil support and staff training.

6. Annual review, testing and assurance
Filtering and monitoring will be reviewed at least annually and after any significant incident or change in guidance. The review will:

- be carried out by SLT, the DSL, OLICAT IT Services and the responsible governor;

- check Securly category settings, HTTPS inspection configuration and alert thresholds for continued appropriateness to our pupils and curriculum;

- include sample checks of alerts, response records and the timeliness/quality of safeguarding follow-up;

- test device off-site protections and resilience to ensure protection settings apply consistently.

- Review outcomes and required actions will be reported to the Local Academy Committee.

7. Limitations and escalation
No technical system removes all risk. Securly significantly reduces risk but cannot prevent every incident. The school therefore combines technical measures with staff supervision, education, robust behaviour expectations and clear acceptable-use policies.

Any technical shortfalls, false negatives/positives or recurring risks identified via Securly are escalated to OLICAT IT Services and the Trust for prompt remediation.

8. Implementation and related documents
This statement sits alongside the school's Child Protection Policy, Acceptable Use Policy and the Trust IT policies. OLICAT IT Services maintains documentation of Securly configuration and change logs. Any change to settings must be authorised by named senior leads.

Sources and statutory alignment: This policy is written to meet the expectations of Keeping children safe in education 2025 (filtering and monitoring requirements, annual review and roles and responsibilities).