St Cecilia's Catholic Primary School

Filtering & Monitoring Policy

"With Jesus as our guide and walking by our side,
we learn to love and love to learn."

Date of policy:	March 2026	Reviewed:	
Signed by:			
S. Hurst	Headteacher	Date:	March 26
J. Kilburn	Co Chair of governors	Date:	March 26
L. Fogherty	Co Chair of governors	Date:	March 26

Contents

1.Statement of intent
2. Legal and Statutory Content
3. Roles and Responsibilities
4.Filtering Arrangements
5. Monitoring Arrangements
6. Responding to incidents
7. Data protection and privacy
8. Education and Training
9. Testing and Review
10. Remote learning
11. Monitoring and Review

1.Statement of intent

This policy explains how St Cecilia's Catholic Primary School uses internet filtering and monitoring systems to:

- Keep pupils safe online
- Prevent access to harmful or inappropriate content
- Support teaching and learning
- Meet statutory safeguarding requirements
- Comply with "Keeping Children Safe in Education" (KCSIE)

It should be read alongside:

- Online Safety Policy
- Safeguarding and Child Protection Policy
- Acceptable Use Policy
- Data Protection Policy

2. Legal and Statutory Content

The school recognises its responsibilities under:

- Keeping Children Safe in Education (KCSIE)
- Prevent Duty Guidance
- UK GDPR and Data Protection Act 2018
- Education Act 2002
- DfE Meeting Digital and Technology Standards in Schools and Colleges (Filtering and Monitoring Standards)

This policy supports the requirement to have:

- Appropriate filtering systems through **Netsweeper (Juniors) Trustnet (Infants)**
- Effective monitoring systems through **Securus**
- Clear roles and responsibilities
- Robust reporting and response procedures

3. Roles and Responsibilities

Governing Body

The Governing Body will:

- Ensure appropriate filtering and monitoring systems are in place
- Review online safety and safeguarding arrangements
- Receive reports on the effectiveness of filtering and monitoring
- Ensure compliance with KCSIE and DfE standards

Headteacher

The Headteacher will:

- Ensure this policy is implemented
- Allocate resources for effective filtering and monitoring
- Support staff training
- Ensure incidents are managed appropriately

Designated Safeguarding Lead (DSL)

The DSL is responsible for:

- Oversight of filtering and monitoring systems
- Acting on safeguarding concerns identified through monitoring

- Keeping records of online safety incidents
- Liaising with Securus where necessary
- Ensuring regular checks of system effectiveness
- Reporting concerns to appropriate agencies when required

Computing Lead

Responsible for:

- Day-to-day management of Securus systems
- Maintaining filtering rules and categories
- Running and reviewing monitoring reports
- Ensuring updates and system health
- Liaising with the DSL regarding concerns

All Staff

All staff must:

- Follow the Acceptable Use Policy
- Supervise pupils appropriately
- Report online safety concerns to the DSL
- Be aware that online activity is monitored
- Model safe and responsible technology use

4.Filtering Arrangements

4.1 Filtering System

St Cecilia's uses **Net sweeper** as its primary filtering, **Trustnet** is used in the Infant building and **Securus** monitoring solution.

These systems provide:

- Web content filtering
- Keyword monitoring
- Real-time alerts
- Screenshot capture
- User activity reporting

- Device and network monitoring

4.2 What is Filtered

The filtering system Net sweeper/ Trustnet is configured to block or restrict access to:

- Adult content
- Extremist material
- Violence and hate
- Gambling
- Social media (unless approved)
- Chat rooms and messaging services
- Malware and phishing sites
- Proxy and VPN services
- Any other content deemed inappropriate for primary-aged pupils

Filtering is applied to:

- All school-owned devices
- The school network
- Guest networks

4.3 Differentiated Filtering

Different filtering levels are applied for:

- Pupils
- Staff
- Administrators

This ensures that:

- Pupils receive age-appropriate access
- Staff can access legitimate teaching resources
- Safeguarding is not compromised
- When Ipads are being used they are not on the same filtering system, so adults must be vigilant and watch pupils closely.

4.4 Requests for Changes to Filtering

If a legitimate website is blocked, staff may request unblocking by:

1. Emailing the hi-impact support
2. Providing the website address and purpose
3. Hi-impact will then ask for approval from the head teacher before access is granted

Any changes must be approved by the DSL or Headteacher.

5. Monitoring Arrangements

5.1 Monitoring System

Securus monitoring software is used to:

- Monitor online searches
- Capture concerning keywords
- Detect inappropriate behaviour
- Identify safeguarding risks
- Record device activity

Monitoring covers:

- Internet searches
- Typed text
- Applications
- Screenshots
- Attempts to access blocked content

5.2 Real-Time Alerts

Securus provides real-time alerts for:

- Self-harm related searches
- Bullying language
- Radicalisation concerns
- Sexual content
- Grooming indicators
- Abusive behaviour

Alerts are automatically sent to:

- Headteacher

- The DSL
- Deputy DSL
- Computing Lead

5.3 Review of Logs

- Monitoring logs are reviewed daily during term time
- High-risk alerts are acted on immediately
- Lower-level concerns are reviewed weekly
- Records/reports are kept securely in line with safeguarding procedures

6. Responding to incidents

6.1 Low-Level Incidents

Examples:

- Accidental access attempts
- Minor misuse
- Inappropriate searches without intent

Response may include:

- Discussion with pupil
- Reminder of online safety rules
- Informing class teacher

6.2 Safeguarding Concerns

If monitoring identifies a safeguarding concern:

- The DSL will be alerted immediately
- The incident will be recorded on the safeguarding system
- Parents/carers may be contacted
- External agencies may be involved where appropriate

6.3 Serious Incidents

Incidents involving:

- Extremism

- Sexual content
- Bullying or harassment
- Threats
- Self-harm concerns

Will be managed in line with:

- Safeguarding Policy
- Behaviour Policy
- Local safeguarding procedures

7. Data protection and privacy

The school recognises that:

- Monitoring is necessary for safeguarding
- Data is processed lawfully and proportionately
- Only authorised staff access monitoring data
- Records are kept securely
- Data is retained in line with school retention schedules

Users are informed through:

- Acceptable Use Policies
- Privacy notices
- Staff induction

8. Education and Training

The school will ensure that:

- Staff receive regular online safety training
- Staff understand Securus alerts and procedures
- Pupils are taught about safe internet use
- Governors receive updates on filtering and monitoring

9. Testing and Review

The effectiveness of filtering and monitoring will be reviewed:

- At least annually
- After any significant incident
- When new guidance is issued
- When systems or providers change

Checks will include:

- Test searches
- Reviewing blocked categories
- Reviewing alert logs
- Confirming staff awareness

10. Remote learning

Where pupils access school systems remotely:

- The same filtering standards will apply where possible
- Securus monitoring will remain active on school devices
- Parents will be supported with online safety guidance

11. Monitoring and Review

The next scheduled review date for this policy is **March 2027.**