



Appendix C – Filtering and Monitoring Arrangements

Bramcote Church of England Primary School (2026–2027)



This appendix should be read alongside the school's Online Safety Policy Child Protection and Safeguarding Policy, Staff Acceptable Use Agreement and Cyber Security Procedures.

Filtering and monitoring arrangements form a key part of the school's safeguarding framework and are implemented in line with KCSIE 2026 and the DfE Filtering and Monitoring Standards which are in process with support from RMG Technologies.

1. Purpose

Bramcote Church of England Primary School uses filtering and monitoring systems to:

- Protect children from exposure to illegal, inappropriate and harmful online content.
- Identify safeguarding concerns at the earliest possible stage.
- Support staff in maintaining a safe and secure digital environment.
- Enable the safe educational use of online technologies.
- Meet statutory safeguarding obligations and DfE filtering and monitoring requirements.

The school recognises that filtering and monitoring support safeguarding but do not replace effective supervision, online safety education, staff vigilance or professional judgement.

2. Scope

These arrangements apply to:

- All pupils.
- All staff, governors, volunteers and visitors.
- All school-owned devices.
- School broadband and wireless networks.
- Cloud-based systems and digital learning platforms.
- Any device authorised to access the school's network or internet services.

3. Roles and Responsibilities

Governing Body

The Governing Body will:

- Ensure effective filtering and monitoring systems are in place.
- Review annual filtering and monitoring reports.
- Provide challenge regarding safeguarding risks identified through monitoring.

- Review compliance with DfE Filtering and Monitoring Standards.
- Receive regular safeguarding updates from the DSL and Headteacher

Headteacher

The Headteacher will:

- Ensure sufficient resources are allocated to filtering and monitoring.
- Ensure systems are reviewed and tested regularly.
- Ensure staff receive appropriate training.
- Support the DSL in responding to incidents and alerts.

Designated Safeguarding Lead (DSL)

The DSL will:

- Lead on safeguarding concerns generated through monitoring systems.
- Review alerts promptly and determine appropriate actions.
- Maintain records of investigations and outcomes.
- Lead the annual filtering and monitoring review.
- Report trends and concerns to governors.

IT Support Provider

The school's IT support provider will:

- Maintain filtering and monitoring systems.
- Ensure systems remain effective and up to date.
- Provide reports and technical support.
- Escalate safeguarding concerns promptly to the DSL.
- Support annual testing and auditing arrangements.

Staff

All staff will:

- Supervise pupils appropriately.
- Report concerns immediately.
- Follow acceptable use expectations.
- Understand monitoring systems and escalation procedures.
- Participate in annual online safety and safeguarding training

4. Filtering Arrangements

The school's filtering systems are designed to:

Block Illegal Content

The system prevents access to:

- Child sexual abuse material (CSAM)
- Terrorist and extremist material
- Criminal content
- Other unlawful material as defined by UK legislation.

Restrict Harmful and Inappropriate Content

Filtering controls reduce access to:

- Pornographic content
- Self-harm and suicide material
- Eating disorder content
- Violent content
- Hate speech and discrimination
- Extremist material
- Gambling websites
- Piracy and copyright infringement sites
- Misinformation and disinformation content
- Unsafe social networking and communication platforms where appropriate.

Age-Appropriate Filtering

Filtering settings are tailored to:

- Primary age pupils.
- Staff access requirements.
- Curriculum and educational needs.

Circumvention Controls

The school takes reasonable steps to prevent bypassing of filtering through:

- VPN services.
- Proxy servers.
- Alternative DNS services.
- Anonymous browsing tools.

5. Monitoring Arrangements

Monitoring systems are used to support the identification of safeguarding concerns including:

- Searches relating to self-harm or suicide.
- Bullying or harassment.
- Extremism and radicalisation.
- Violence.

- Child-on-child abuse.
- Sexual harassment.
- Harmful online behaviour.
- Attempts to bypass filtering systems.
- Unauthorised access activities.

Monitoring includes:

- Technical monitoring software.
- Network activity reporting.
- Device management systems.
- Physical supervision by staff.
- Manual review where concerns arise.

All monitoring alerts are subject to human review and professional judgement before safeguarding decisions are made.

6. Responding to Alerts

Where alerts or concerns are identified:

Low-Level Concerns

Examples:

- Accidental access attempts.
- Isolated inappropriate searches.
- Minor breaches of acceptable use.

Response:

- Discussion with pupil.
- Reminder of expectations.
- Recording where appropriate.

Safeguarding Concerns

Examples:

- Repeated concerning searches.
- Self-harm indicators.
- Sexual content searches.
- Bullying or coercive behaviour.
- Extremist content.

Response:

- Immediate referral to DSL.
- Review of context and risk.
- Recording on safeguarding systems.
- Contact with parents where appropriate.
- Referral to external agencies if required.

Serious or Illegal Concerns

Examples:

- Suspected CSAM.
- Terrorist content.
- Grooming.
- Serious cybercrime.

Response:

- Preserve evidence.
- Do not investigate independently.
- Immediate DSL notification.
- Police and safeguarding referral as required.

7. Monitoring of School Devices

All school-owned devices are subject to filtering and monitoring:

- On the school site.
- During educational visits where connected.
- When used remotely.
- When staff work from home using school systems.

Users are informed through:

- Online Safety Policy.
- Acceptable Use Agreements.
- Staff induction.
- Pupil education programmes.

8. Annual Review Process

An annual review of filtering and monitoring effectiveness will be completed by:

- Headteacher.
- Designated Safeguarding Lead.
- IT Support Provider.
- Online Safety Governor.

The review will include:

- Testing filtering effectiveness.
- Testing on different devices.
- Testing in different locations.
- Review of safeguarding alerts.
- Review of incidents and trends.
- Staff and governor discussions regarding effectiveness.

Review records will include:

- Date tested.
- Devices tested.
- Locations tested.
- Issues identified.
- Actions taken.

9. Staff Training

All staff will receive annual training on:

- Online safety.
- Safeguarding responsibilities.
- Filtering and monitoring expectations.
- Reporting procedures.
- Emerging online risks.
- Appropriate use of AI and digital technologies.

Governors involved in safeguarding and online safety will receive additional training to enable effective oversight of filtering and monitoring arrangements.

10. Review

This appendix will be reviewed annually or sooner if:

- Legislation changes.
- DfE guidance changes.
- New technologies are introduced.
- Significant safeguarding concerns arise.
- Filtering or monitoring systems are changed.

Approved by Governing Body: October 2026

Review Date: September 2027

Appendix C1 – Filtering and Monitoring Arrangements (Bramcote Church of England Primary School).

For inclusion within your **Appendix C1 – Filtering and Monitoring Arrangements**, it is helpful to provide staff with clear examples of what constitutes a low-level concern versus a serious safeguarding concern. The examples below are suitable for a primary school context and align with the safeguarding-led approach described in your Online Safety Policy and filtering/monitoring procedures.

Examples of Low-Level Monitoring Alerts

These incidents may not indicate immediate safeguarding risk but should be reviewed, recorded where appropriate, and addressed through education, supervision or behaviour management.

Low-Level Concerns

- Accidental access to inappropriate websites.
- Searches for age-inappropriate content arising from curiosity rather than intent.
- Repeated attempts to access blocked gaming websites.
- Attempts to stream unauthorised videos during lesson time.
- Use of inappropriate language in shared documents or online platforms.
- Attempting to access social media platforms during the school day.
- Minor breaches of the Acceptable Use Agreement.
- Searching for topics linked to violence or weapons without evidence of harmful intent.
- Attempting to bypass age restrictions on educational websites.
- Sharing passwords with friends.
- Excessive internet use unrelated to learning.
- Accessing unauthorised online games.
- Repeated accidental triggering of filtering alerts.
- Attempting to download software or browser extensions without permission.
- Use of AI tools without staff authorisation.

Suggested Response

- Staff discussion with pupil.
- Reinforcement of online safety expectations.
- Reminder of acceptable use rules.
- Monitoring for patterns or repetition.
- Informing parents if concerns become recurring.

Examples of Serious Monitoring Alerts

These alerts may indicate a safeguarding risk and require immediate review by the DSL.

Serious Safeguarding Concerns

Risk of Harm to Self

- Searches about self-harm.
- Searches relating to suicide methods.
- Repeated searches around eating disorders.
- Accessing content promoting self-injury or harmful challenges.

Child Protection Concerns

- Searches concerning child sexual abuse material.
- Searches relating to grooming or exploitation.
- Attempts to access adult pornography.
- Searches for sexual violence or sexually explicit material.
- Evidence of sharing or requesting indecent images.

Extremism and Radicalisation

- Repeated viewing of extremist content.
- Searches supporting terrorism.
- Accessing radicalisation materials.
- Interest in violent extremist groups.

Child-on-Child Abuse

- Sexual harassment or abuse-related searches.
- Discriminatory or misogynistic content.
- Evidence of cyberbullying.
- Threatening online messages.
- Sharing humiliating or abusive content about another pupil.

Criminal or High-Risk Behaviour

- Attempts to bypass filtering through VPNs or proxy services.
- Evidence of hacking tools or cybercrime activity.
- Searches for illegal drugs.
- Searches relating to weapons or violent attacks.
- Fraud, phishing or identity theft activity.

AI-Related Safeguarding Concerns

- Use of AI to create harmful content.
- Use of AI image-generation tools to create inappropriate images.
- Attempts to access age-inappropriate AI companions or chatbots.
- AI-generated bullying, harassment or impersonation of others.

Immediate DSL Referral Required

Staff should refer concerns immediately where monitoring identifies:

- Self-harm or suicide indicators.
- Sexual exploitation concerns.
- Grooming indicators.
- Child-on-child sexual abuse.
- Extremism or radicalisation.
- Criminal activity.
- Serious cyberbullying.
- Any pattern suggesting a pupil may be at risk of significant harm.

Examples of Illegal Content Requiring Immediate Escalation

- Child sexual abuse material (CSAM).
- Terrorist material.
- Criminal exploitation content.
- Serious cybercrime activity.
- Evidence of grooming or exploitation.

These matters should be referred immediately to the DSL and, where necessary, police or external safeguarding agencies. Staff should preserve evidence and not undertake their own investigation.

Examples of Monitoring Alerts and Escalation Thresholds

Monitoring Alerts: Escalation Thresholds

All monitoring alerts are reviewed in context. A single alert may not indicate a safeguarding concern; however, patterns of behaviour, repeated alerts, pupil vulnerability factors and wider safeguarding information will always be considered when determining risk and appropriate action.

Table 1: Low-Level Monitoring Concerns

Category	Examples of Monitoring Alerts	Typical Response
Website Access	Accidental access attempts to blocked websites	Staff discussion and reminder of expectations
Searching	Isolated age-inappropriate searches arising from curiosity	Online safety education and monitoring
Games & Entertainment	Attempts to access gaming or streaming sites during lesson time	Behaviour intervention and supervision
Social Media	Attempts to access social media platforms during the school day	Reminder of acceptable use expectations
Device Use	Downloading unauthorised apps, software or browser extensions	Investigation and removal of software where required

Account Security	Sharing passwords with friends	Education regarding online security
Online Conduct	Inappropriate language in shared documents, emails or collaborative platforms	Behaviour sanction and restorative discussion
AI Use	Use of unapproved AI tools without staff permission	Education regarding safe and authorised use
Filtering Alerts	Repeated low-risk filtering alerts without safeguarding indicators	Monitoring and review
Acceptable Use	Minor breaches of the Acceptable Use Agreement	Recorded and addressed through behaviour procedures

Typical Actions for Low-Level Concerns

- Discussion with the pupil.
- Reinforcement of online safety expectations.
- Reminder of acceptable use rules.
- Increased supervision or monitoring where appropriate.
- Recording where patterns of behaviour emerge.
- Parent communication if concerns are repeated.

Table 2: Serious Monitoring Concerns Requiring DSL Review

Category	Examples of Monitoring Alerts	Required Response
Self-Harm	Searches relating to self-harm, suicide or eating disorders	Immediate DSL referral and safeguarding assessment
Sexual Content	Attempts to access pornography or sexually explicit material	DSL investigation and safeguarding response
Child Protection	Searches relating to child sexual abuse material (CSAM)	Immediate DSL referral and potential police involvement
Grooming & Exploitation	Activity indicating grooming, coercion or exploitation	Immediate safeguarding referral
Child-on-Child Abuse	Sexual harassment, coercive behaviour or abusive online conduct	DSL investigation and risk assessment
Cyberbullying	Serious bullying, threats or targeted harassment	Safeguarding response and parental involvement
Extremism	Searches or access to extremist or radicalising content	Immediate DSL review and Prevent consideration
Violence	Searches relating to weapons, violent attacks or serious harm to others	DSL assessment and possible external agency involvement
Illegal Activity	Drug-related content, fraud, phishing or criminal activity	Immediate escalation and investigation
Hacking & Circumvention	Use of VPNs, proxies, hacking tools or attempts to bypass filtering	DSL and IT provider review

AI Misuse	Creation of harmful, abusive or inappropriate AI-generated content	Safeguarding investigation
Repeated High-Risk Alerts	Persistent concerning searches or activity over time	Immediate safeguarding intervention

Immediate DSL Escalation

The following incidents should always be treated as high-risk safeguarding concerns:

- Child Sexual Abuse Material (CSAM).
- Grooming or child exploitation.
- Serious self-harm or suicide indicators.
- Extremist or terrorist content.
- Serious cybercrime activity.
- Online sexual abuse or image-sharing offences.
- Threats of significant violence to self or others.

Where appropriate, external agencies including MASH, Police, Prevent, CEOP or other safeguarding partners will be informed in accordance with the Child Protection Policy. Staff must preserve evidence and should not undertake their own investigation.