

Greenfields Community School

Information Monitoring and Filtering Policy



September 2026

Document Origins		
Version Date	Review date	Approval date
September 2025	September 2026	FGB 09/25
September 2026	September 2027	FGB

Document Version History		
Revision date	Author of changes	Summary of changes
Sept 2026	Lou Maltby (HT)	Updated to reflect Keeping Children Safe in Education document 2026

Greenfields Community School is committed to safeguarding and promoting the welfare of all pupils. The school recognises that technology plays a vital role in education and that access to digital resources enhances teaching, learning and communication. However, the use of technology also presents potential risks.

The purpose of filtering and monitoring is to support safeguarding by reducing the likelihood of pupils accessing harmful or inappropriate content and by identifying behaviours that may indicate a safeguarding concern. Filtering and monitoring form part of the school's wider safeguarding responsibilities and should be read alongside the Safeguarding and Child Protection Policy, Online Safety Policy, Behaviour Policy and Acceptable Use Agreements. The school follows the requirements set out within Keeping Children Safe in Education 2026 and the Department for Education's filtering and monitoring standards.

1. Purpose

This policy aims to:

- Safeguard pupils from exposure to illegal, harmful, inappropriate or age-inappropriate online content. [\[gov.uk\]](https://www.gov.uk)
 - Support the identification of safeguarding concerns through appropriate monitoring arrangements. [\[gov.uk\]](https://www.gov.uk), [\[saferinternet.org.uk\]](https://saferinternet.org.uk)
 - Protect the school's network, devices and information systems from security threats and cyber-attacks. [\[gov.uk\]](https://www.gov.uk)
 - Promote safe, responsible and ethical use of technology.
 - Ensure compliance with statutory safeguarding requirements and data protection legislation.
 - Establish clear roles, responsibilities and procedures regarding filtering and monitoring arrangements.
-

2. Scope

This policy applies to:

- All pupils.
- All staff.
- Governors.
- Volunteers.
- Contractors.

- Visitors using school networks or devices.

The policy covers:

- School-owned devices.
 - School networks and internet services.
 - School email accounts.
 - Cloud-based services.
 - Any authorised personal devices accessing school systems.
-

3. Roles and Responsibilities

3.1 Governing Body

The Governing Body will:

- Ensure appropriate filtering and monitoring systems are in place.
- Review filtering and monitoring arrangements regularly.
- Ensure safeguarding responsibilities are met.
- Receive updates regarding online safety and filtering arrangements.

3.2 Headteacher

The Headteacher will:

- Ensure this policy is implemented effectively.
- Ensure appropriate resources are available.
- Oversee investigations arising from monitoring alerts.
- Report significant concerns to governors where appropriate.

3.3 Designated Safeguarding Lead (DSL)

The DSL will:

- Take lead responsibility for online safeguarding.
- Understand the filtering and monitoring systems in operation.
- Review safeguarding alerts and monitoring reports.
- Ensure concerns are recorded and acted upon appropriately.
- Liaise with external agencies where necessary.

3.4 IT Support Provider

The school's IT support provider will:

- Maintain filtering and monitoring systems.
- Ensure systems remain effective and secure.
- Support investigations where required.
- Provide reports and technical information when requested.

3.5 Staff

All staff will:

- Supervise pupils' online activity appropriately.
- Report safeguarding concerns immediately.
- Follow the school's Acceptable Use Agreements.
- Participate in relevant safeguarding and online safety training.

4. Filtering Arrangements

Greenfields Community School uses:

- **Smoothwall Monitor**
- **Netsweeper Filtering**

to provide age-appropriate filtering and monitoring of internet activity.

Filtering systems are designed to:

- Block access to illegal content.
- Restrict access to inappropriate content.
- Prevent access to harmful material.
- Support compliance with safeguarding requirements.
- Reduce access to content that may present safeguarding concerns.

Filtering will seek to restrict access to:

- Child sexual abuse material.
- Extremist and terrorist content.
- Pornographic material.
- Violence and graphic content.
- Self-harm and suicide-related content.

- Hate content.
- Criminal activity.
- Gambling.
- Malware and malicious software.
- Content considered inappropriate for pupils.

Filtering arrangements will be reviewed regularly to ensure continued effectiveness.

5. Monitoring Arrangements

Monitoring helps identify safeguarding concerns and inappropriate use of technology.

Monitoring may include:

- Websites visited.
- Search activity.
- Device activity.
- User logins.
- Attempts to bypass school filtering.
- Potential indicators of cyberbullying.
- Potential safeguarding concerns.

Smoothwall systems generate alerts where concerning activity is identified.

Monitoring is undertaken to:

- Safeguard pupils and staff.
- Protect school systems.
- Support investigations where necessary.
- Meet statutory safeguarding obligations.

Monitoring does not replace active staff supervision of pupils.

6. Artificial Intelligence (AI)

The school recognises that AI technologies are increasingly used within educational settings.

Filtering and monitoring arrangements will take into account the safeguarding risks associated with AI-generated content and AI-enabled platforms.

Pupils and staff must:

- Use approved AI technologies responsibly.
- Verify AI-generated information before use.
- Not input confidential, personal or safeguarding information into AI systems.
- Follow school guidance regarding acceptable use of AI.

Please see AI Policy Feb 2026

7. Responding to Monitoring Alerts

Where filtering or monitoring systems identify concerning activity:

1. The alert will be reviewed by an appropriate member of staff.
2. Safeguarding concerns will be referred to the DSL immediately.
3. All actions will be recorded where appropriate.
4. Parents/carers may be informed where necessary.
5. External agencies may be contacted if required.

Serious concerns may include:

- Attempts to access illegal content.
- Radicalisation concerns.
- Child exploitation concerns.
- Cyberbullying.
- Self-harm indicators.
- Repeated attempts to circumvent filtering controls.

8. Reporting Concerns

Any member of the school community who becomes aware of:

- Inappropriate content.
- Safeguarding concerns.
- Security incidents.
- Attempts to bypass filtering controls.

must report the concern immediately to the DSL or Headteacher.

Where necessary, referrals may be made to:

- Children's Social Care.
- Police.
- CEOP.
- Internet Watch Foundation (IWF).
- Other relevant safeguarding agencies.

9. Training

The school will provide regular training to staff on:

- Online safety within Annual Safeguarding Training
- Filtering and monitoring systems within Annual Safeguarding Training
- Cyber security awareness.
- Emerging technologies and risks.
- AI-related safeguarding issues within Annual Safeguarding Training
- Reporting procedures.

Pupils will receive age-appropriate online safety education through the curriculum and wider safeguarding programme.

10. Data Protection and Privacy

Monitoring activities will be conducted lawfully and proportionately.

The school will:

- Comply with UK GDPR.
- Comply with the Data Protection Act 2018.
- Ensure information obtained through monitoring is handled securely.
- Restrict access to monitoring information to authorised personnel only.

Individuals should be aware that use of school networks, systems and devices may be monitored for safeguarding and security purposes.

11. Policy Review

This policy will be reviewed annually by:

- The Headteacher.
- The Designated Safeguarding Lead.
- The Governing Body.

The policy may be reviewed earlier in response to:

- Changes in legislation.
- Changes in technology.
- Significant safeguarding incidents.
- Updated DfE guidance.